김일성종합대학출판사
주체91

정보보안관리

편 람

김일성종합대학출판사

차 례

제１０장. Checkpoint방화벽 보안점검을 어떻게 할것인가

제１１장. 방화벽기술비교

제１２장. 가상개별망의 보안

제１３장. 전자우편보안

제14장. 쿠키와 Web Bug란 무엇인가

제15장. 가상개별망의 실현

제16장. 무선국부망보안

제3편. 보안관리실천

제17장. 경영진의 공약유지

제18장. 보안의식의 계발

제１９장. 보안의식의 계발: 부록

제２０장. 방책개발

제２１장. 신뢰문제

제２２장. 위험관리와 분석

제２３장. 정보위험관리의 새로운 추세

제24장. 기업내 정보보안

제25장. 기업보안정보관리

제26장. 구성관리

제4편. 응용 및 체계개발 보안

제27장. Web응용보안

제２８장. 확고한 보안: 새로운 보안세계질서

제２９장. XML과 기타 메타 자료언어에 대한 보안

제３０장. XML과 정보보안

제３１장. 관계형자료기지 응용에서의 수자식서명

제３２장. 자료보관고의 보안과 사적비밀

제５편. 암호기법

제３３장. 선진암호화표준(AES)에 대한 고찰

제３４장. 공개열쇠계층구조의 보호

제６편. 보안구성방식과 모형

제３５장. 자료기지의 무결성에 관한 고찰

제７편. 운영보안

제３６장. 지능침입분석

제３７장. 전자상업거래환경의 검토

제８편. 업무지속성계획화와 재해복구계획화

제３８장. 업무지속성계획화 공정의 재구성

제３９장. 업무재개의 계획화와 재해복구: 사실자료

제９편. 법, 조사 및 륜리

제４０장. 무슨 사건인가

제４１장. 인터네트불평싸이트와 밸리 대 페이버사건

제４２장. 비요청전자우편에 대한 통제

제１０편. 물리적보안

제４３장. 물리적보안은 정보보안의 기초

제４４장. 물리적보안

머 리 글

기술은 말그대로 놀라운 속도로 발전하고 있다. 그에 따라 정보보안관리를 담당한 전문가들앞에는 여러가지 난문제들이 매일 매 시각 제기되고 있다. 그러므로 우리는 장별로 새로운 경향, 새로운 개념, 보안방법론들이 제시되여 있는 《정보보안관리편람》제4판 3권을 내놓게 된다. 우리는 이 책이 정보보안에 관심이 있는 전문가들의 실천에서 언제나 쓰일수 있는 최신참고서가 되리라고 믿는다.

우리는 또한 정보보안전문가들에게 CISSP시험에 응시하기 위하여 《정보보안일반지식》(CBK)을 이 《정보보안관리편람》의 내용과 함께 볼것을 권고한다. 국제정보체계보안인증협회가 주관하는 CISSP시험제도와 CBK토론회는 전 세계적으로 진행될뿐아니라 그 요구도 매우 높다.

이 시험에 응시하자면 CBK에 담겨 져 있는 많은 문제들도 전반적으로 리해하고 적용해야 하므로 상당한 노력이 든다. 《정보보안관리편람》계렬의 도서들은 이 CISSP자격시험에 응시하려는 사람들에게 가장 중요한 참고서로 인정되고 있다. 이 도서들은 또한 실지 사업에서 여기에 담겨 진 내용들을 정상적으로 응용하려는 전문가들과 비전문가들에게도 쓸모 있을것이다.

끊임없이 증식되는 콤퓨터비루스와 웜들, 공개망규약에서 보안상의 빈 구석들을 살살이 찾아 내는 악질적인 해커들의 계속되는 위협으로 말미암아 최고경영자는 기업재산을 보호하려고 책임성을 가지고 최상의 자격들을 갖춘 보안전문가를 부지런히 찾지 않으면 안되게 된다. 그러므로 CISSP자격은 그 어느 때보다도 필수적인것으로 된다고 보아 진다.

그런 의미에서《정보보안관리편람》의 본판과 후판들의 차례는 CISSP자격시험의 분야에 맞게 편성되여 있다. 매 도서들의 매개 장들에서는 넓은 범위의 정보보안분야와 관련된 CBK에서 제기되는 론점들을 다루고 있다. 그러므로 매판에서 100% 새로운 장들을 담음으로써 이 분야의 발전추세에 맞게 최신내용들을 반영하려고 하였다. 이전 판들과 반복된 장은 하나도 없다.

제 1 편
접근조종체계와 방법론

정보는 귀중하며 따라서 그것이 오용되거나 공개되거나 파괴되지 않도록 하여야 한다는 인식으로부터 출발하여 각 기관들에서는 그에 대한 접근조종을 실시하여 결심채택에 필요한 결정적인 정보들이 그 무결성과 안전성을 잃지 않도록 적극 노력하고 있다.

이 편에 나오는 장, 절들에서는 사용자식별 및 인증, 접근조종기법들과 이 기법들의 적용 그리고 그 조종에 맞서는 새로운 공격방법들에 대하여 서술하였다.

생체계측학이 개인들을 식별하고 보증하며 정보에 대한 접근을 조종하기 위한 수법으로서 광범위하게 리용되고 있는것은 이 생체계측학적수법들이 사람의 음성, 손자리, 지문 혹은 망막모양새 등과 같은 개체적특성을 가지고 사람을 식별할수 있는 가능성을 제공하기때문이다. 생체계측학적수법들이 나온지는 몇해 안되지만 혁신적으로 새로운 안들이 계속 제기되고 있다. 이 중요한 수법들이 가지고 있는 잠재력은 물론 제한성까지 잘 알아야 이 기술을 정확히 그리고 효과적으로 적용할수 있을것이다.

환자의 건강정보의 개인성, 비밀성, 안전성을 보호하는데서만큼 접근조종이 절실히 필요한 분야는 아마 없을것이다. 북아메리카주를 내놓고 특히 유럽나라들에서는 오래동안 인간의 개인성문제가 상당히 우선시되여 왔다. 최근에 와서 국내소비자들은 자기들의 개인자료들이 보호되고 있다는 확고한 담보를 요구해 나서는데 이르게 되였다. 이 요구는 그들의 건강정보가 점점 더 퍼지게 되여 심각한 정도로 로출될수 있다는 우려를 반영하는것이다. 1996년에 통과된 《건강보험공용 및 책임관계법》(HIPAA: The Health Insurance Portability and Accountability Act)과 1999년에 발표된 《그램-리취-블릴리법》(Gramm-Leach-Bliley Act)만 보아도 정부가 국민들의 요구에 매우 조심스러운 태도를 보이고 있었다는 명백한 증거로 된다.

나쁜 마음으로 해킹하는자들이 있음으로 하여 정보조종은 크게 뒤흔들리게 되고 정보보안은 심각한 위협에 계속 직면하고 있다. 해커들은 대체로 기관들이 구축한 방어체계에 조금씩 뚫고 들어 가 못 쓰게 만드는데 그것이 성공한 실례는 너무나도 많다. 이 편에서는 최근에 법무성 Web싸이트를 망신시키고 여러 상업싸이트에 봉사거부공격을 가했다고 굉장히 보도된 해커들의 정교한 공격도구들에 대하여 설명한다.

사회공학적수법들은 인간의 심리를 리용하는 방법으로 설치해 놓은 통제장벽을 뚫는 하나의 방법으로 된다. 사회공학이라는것은 비량심적인 사람들이 우회적인 경로를 리용하여 남이 구축해 놓은 조종망들을 파괴할수 있는 정보들을 얻어 내는것을 말한다. 실례로 콤퓨터기술자로 가장한 어떤자가 불의에 한 콤퓨터사용자에게 전화를 걸어 망에서 기술적으로 문제가 생겨 고쳐야 하겠으니 당신의 망통과암호를 알려 달라고 해서 그 암호를 가지고 그 체계를 쭉 해결해 치우는것을 볼수 있다.

제1장. 생체계측학에서 새로운 점

쥬디스 엠 마이어슨

망세계에서의 안전문제는 오래동안 통과암호나 개인식별번호(PIN) 혹은 자기 어머니의 애명과 같은 개인정보에 의거하여 왔다. 지금 이런것들은 카드열쇠, 스마트카드, 토큰열쇠와 함께 생체계측지표로 보강되고 있다. 생체계측학에서는 사람의 손끝, 눈, 얼굴특징들을 계측한다. 사람이 말은 어떻게 하며 열쇠는 어떻게 매만지며 걸음은 어떻게 걷는가에 의해서도 계측될수 있다. 앞으로는 사람의 귀가 어떻게 생겼으며 소리를 어떻게 듣는가에 대해서도 사람별로 측정할수 있을것이다.

전통적인 생태계측체계를 본 다음 보다 새로운 기술과 체계를 보라. 표준화문제와 설정기준만 간단히 토론하면 즉시 새 기술로 되는것이다.

지 문

검은잉크판대기에 시끄럽게 손가락을 굴려 지문을 따고 또 흰종이에 복사하기를 며칠 하는 지문채취작업은 몇년만 있으면 과거의 일로 될것이다. 이제 마음 먹은대로 그 무슨 일이나 다 할수 있는 지문수감기의 시대에 들어 가게 된다. 손가락끝을 지문수감기의 수감소편우에 슬쩍 놓으면(재빨리 그리고 깨끗이) 먼 곳에 있는 망체계에 쉽게 접근할수 있을것이다. 같은 지문은 없으니 내 지문은 복제 못할것이라고 안심을 할수 있을것이다.

지문은 손가락끝에 있는 무늬들의 모임이다. 잘 찍은 지문은 끊긴 선들과 가지 친 선들로 되여 있다. 이것을 지문색인에서는 세밀선이라고 한다. 보통 지문 한개에는 40～60개의 세밀선이 있다. 무늬들이 세밀선이 보일 정도로 되여도 수감기들은 손가락끝의 모든 세부들을 다 포착 못할수도 있다. 일부 사람들의 손가락무늬들은 타자를 너무 치거나 힘든 고전곡목들을 피아노연주하여 너무 희미해짐으로써 잘 보이지 않는 경우들도 있다. 또한 날 때부터 유전적결함이 있거나 사고로 손가락끝에 상처가 있든가 하면 지문읽기가 매우 힘들것이다.

이미 보관되여 있는 지문기록과 개인들의 지문을 대조해 보는 방법에는 4가지 즉 전자수감, 온도수감, 광학수감, 혼성수감이 있다. 전자수감에서는 지문의 마루와 골짜기사이의 전자기마당세기의 변화를 측정한다. 온도수감에서는 손가락누름새 즉 수감부표면을 지나갈 때 손가락끝표면의 마루들이 마찰로 하여 비접촉골보다 더 열을 발산하는 특성으로부터 생기는 온도차를 측정한다. 광학수감에서는 지문의 파장차이를 측정한다. 혼성수감에서는 광학수감과 전자수감을 혼성하는 방법을 리용한다.

눈 알 스 캔

지문에서와는 달리 사람의 눈에는 그 구조상 세밀선들이 수천개나 된다. 지문세밀선들은 지문의 외적구조의 무늬밖에 보여 주지 못하지만 사람의 눈에 있는 세밀선들은 눈알의 내적구조의 무늬까지 보여 준다. 이러한 눈정보는 두가지 즉 망막스캔체계와 홍채스캔체계로 얻을수 있다. 망막스캔은 망막에 있는 정맥분포형태를 포착할수 있다면 홍채스캔으로는 홍채의 섬유와 조직, 고리형태들을 얻어 낸다.

망막스캐너는 세기가 낮은 광원을 광학결합기에서 발산하여 해당 인원의 고유한 망막형태를 얻어 낸다. 이러한 스캐너를 리용하자면 사람이 시창구를 들여다 보면서 동시에 눈이 일정한 곳에 초점을 맞추어야 하는데 이렇게 되면 시력교정렌즈인 접안렌즈를 끼고 있는 사람들이나 어떤 기구와 접촉하면 불안해 하는 사람들의 경우 스캔효과가 과연 정확하게 나오겠는가 하는 문제가 제기된다.

홍채스캐너는 보통 TV카메라 같은 기구를 쓰므로 가깝게 접촉하지 않아도 된다. 홍채측정값들은 접안렌즈나 안경 같은것을 끼고 있어도 조명도만 좋으면 일 없다.

병이나 외상으로 인하여 시간이 지나면 눈정보가 달라 질수 있다는것도 알아야 한다. 눈알스캔은 맹인들에게 필요 없다. 또한 시력장애가 있는 사람들 특히 망막이 손상된 사람도 쓸 필요가 없다.

얼 굴 인 식

얼굴인식체계를 리용하면 TV방영, 건물이나 거리를 감시하는 유선카메라에 비치는 사람들의 얼굴들을 자동적으로 인식할수 있다. 하나의 새로운 어떤 체계에서는 어둠속에서 가동하면서 대상인물의 얼굴에서 나오는 적외선열을 추적하여 현시하기도 한다. 도박산업에서는 오래전부터 얼굴인식체계망을 독점적으로 리용하여 사기군들의 얼굴을 자료기지화해 놓음으로써 보안경찰이 인차 잡아 낼수 있게 하고 있다.

만일 모양이 완전히 달라 졌을 경우 례하면 코수염을 길렀든가 아니면 괴상한 표정을 짓고 있다든가 하는 경우에는 얼굴인식체계에 혼란이 조성될수 있다. 또한 카메라와 해당 인물의 얼굴각도가 완전히 달라 져도 체계에 혼란이 일어 나게 된다. 자료기지에 입력된 영상과 문제의 영상사이의 위치차가 15° 만 되여도 부정적판별이 나오게 된다. 따라서 45° 의 차이에서는 인식이 불가능해 진다.

손과 음성

손의 기하학적생김새를 기록해 두는것은 옛날부터 감옥에서 많이 써왔다. 말하자면 손가락들의 길이, 너비, 굵기와 곡선생김새와 정맥 등 기타 특징들을 비롯하여 손

의 3차원적특성들을 리용한다는것이다. 이때 부은 부위나 유전적변형도 놓치지 말아야 한다.

음성정보기록을 유럽에서는 전화리용에서 많이 쓴다. 겨울에는 손이 시려 장갑을 끼기때문에 전화 거는 사람들의 손기록보다 음성정보가 더 편리하다. 사고나 병, 년로로 하여 목소리가 나쁜것은 물론 주변소음준위가 높을 때에는 음성검증이 상당히 곤난하다.

새로운 점은 무엇인가

최근에 생체계측학적수법들은 감옥면회자검증체계에서 리용되여 신원을 가장한 면회자를 잡아 내는데 그리고 리득금지불체계에서 사기적인 청구자들을 방지하는데도 사용되여 왔다. 생태계측체계가 구축된것은 또한 화물자동차운전수들이 여러개의 운전면허증을 해가지고 국경이나 주경계선을 넘을 때 고쳐 써가지고 다니는것을 막자는데도 목적이 있다. 새로운 국경통과체계에서는 지정된 생체계측장소들에서 입국하고 출국하는 려행자들을 감시하고 있다. 선거에서는 생체계측학적체계를 리용하여 투표자의 신원을 확인함으로써 대리투표를 막는데 이 체계는 아직 대중화되지 못하고 있다.

그렇다면 무엇이 새로운 점인가, 특히 2001년 1월 1일부터 시작된 세번째 천년기에 들어 와서 말이다. 현황에 대한 간단한 개괄을 위하여 부분적이나마 다음의것들을 소개해 본다.

- 얼굴, 음성과 입술놀림의 결합
- 착용형생체계측기구들
- ATM(자동현금입출기)에 붙은 지문검출소편
- 개인인증
- 기타

이러한 일부 생체계측학적시도들은 이미 시장실현단계에까지 도달하였으나 일부는 아직 연구단계에 있다. 마이크로쏘프트회사는 자체의 생체계측연구계획을 추진시킴으로써 생체계측학적통합에 강한 추동력으로 부상하고 있다.

얼굴, 음성 및 입술놀림의 통합

이 첫 문제는 매우 흥미 있는 문제이며 특히 독순(입술놀림의 읽기)법이라는 계측법은 강한 흥미를 자아낸다. 보다 흥미 있는것은 독순법과 얼굴, 음성을 일체적으로 결합시키는것이다. 이 체계의 우점은 세가지 구성요소중 하나의 방식이 효과가 낮아도 다른 두

가지의 방식이 앞의 낮은 효과를 상쇄, 다시 말하여 하나의 방식이 교란되여도(실례로 음성에서 나오는 잡음환경) 다른 두 방식들을 리용하여 정확한 식별이 가능하다는것이다.

이러한 실례는 Dialog Communications Systems(도이췰란드의 에를랑겐)가 개발한것으로 알려 진 다중생체계측식별체계(Multimodal Biometric Identification System)의 하나인 BioID를 들수 있다. 이 체계에서는 얼굴, 음성, 입술놀림인식을 다 결합하고 있다. 이 체계는 기록자료들을 읽어 들이고 매 생체계측특성들을 따로따로 처리하는것으로 시작한다. 체계의 훈련(자료등록)과정에 생체계측모형들이 매 특성에 한하여 생성된다. 그다음 이 체계는 이 모형들과 새롭게 기록된 형태를 비교하며 결과값들을 종합하여 사람인식에 리용하게 된다.

이 BioID체계는 화상흐름에서 나타나는 한 영상의 국부적움직임과 그다음 부분과의 관계를 보여 주는 벡토르마당값을 계산하는 기법인 빛흐름기법을 리용하여 입술의 놀림새를 포착한다. 이 과정처리를 위하여 전처리구간에서 화상흐름의 처음 17개의 영상중에서 입술부분을 따낸다. 다음 16개의 벡토르마당에서의 입술놀림새정보를 따내는데 이것이 바로 프레임별 입술의 운동인것이다. 목소리를 듣지 않고 입술을 판독하는데서 제기되는 하나의 문제점은 두세개의 각이한 단어들을 발음할 때 같은 입술움직임을 보일수 있다는것이다.

그 회사는 BioID체계가 콤퓨터망, 인터네트상 거래와 은행업무체계 그리고 자동현금입출기 등 그 어느 기술체계에 대한 접근조종에 다 리용할수 있다고 장담하고 있다. 적용분야에 따라 BioID는 개인식별도 할수 있고 검증도 할수 있게 한다. 식별방식에서는 이 체계가 자료기지전체를 검색하여 개체를 식별해 주며 검증방식에서는 사람이 자기의 이름이나 번호를 주면 이 체계가 자료기지의 해당 구역에서 직접 검색하여 생체계측학적 지표들을 확인하는 식으로 검증해 준다.

착용형생체계측체계

오늘날 카메라와 마이크는 매우 작고 가벼워 얼굴식별과 같은데 쓰이는 착용형체계와 성과적으로 결합하여 리용되고 있다. 얼굴식별쏘프트웨어보다 훨씬 더 좋은것이 있는데 그것은 자기의 안경에 음성발신카메라를 장착하는것이다. 이 기구를 리용하면 그 누구를 보는 순간 이 기구가 귀에 누구라고 속삭여 주므로 그 인물이름을 기억해 낼수 있다. 어떤 나라에서는 국경경비대에서 쓸수 있게 이러한 기구들을 많이 시험하였다. 로체스터종합대학 미래건강쎈터의 연구사들은 이런 기구들을 알쯔하이머병을 앓는 환자들에게 쓸것으로 전망하고 있다.

예상해 보건대 다음세대인식체계는 사람들을 보다 쉬운 환경에서 실시간적으로 인식하게 될것이다. 실시간적으로 동작하는 체계들은 세가지 방식에 한정되여 동작하는 우에서 본 체계들보다 훨씬 효률적이다. 때가 오면 그 체계는 두가지이상이 아니라 다만 하나의 생체계측항목으로 인물식별능력을 가지게 될것이다.

ATM카드에 달린 지문수감소편

대부분의 중요은행들은 카드를 도난 당하였을 때 제기되는 신원협잡을 막기 위해 ATM기계에 생체계측을 도입하기 위한 시험을 꾸준히 진행하여 왔다. 그 한 실례는 ATM에 지문수감소편을 장치하는것이다. 일부 회사들은 ATM카드에 생체계측장치와 함께 PKI(공개열쇠기반)를 적용할것을 예견하고 있다. PKI는 사용자식별과 인증에 공개열쇠암호화를 리용하는것이다. 비밀열쇠는 ATM카드에 보관되고 생체계측지표에 의하여 보충되게 된다. 공개열쇠기반이 수학적으로 볼 때 안정성이 더 크지만 그 기본약점은 사용자의 비밀열쇠의 비밀성을 보장해야 하는것이다. 안전하자면 비밀열쇠는 반드시 손상됨이 없이 보호되여야 하는것이다. 방도로는 비밀열쇠를 스마트카드에 넣고 그것을 하나의 생체계측지표로 보호잠금해 놓는것이다.

2001년 1월 18일 Keyware회사(생체계측 및 중앙인증방안들을 제공하는 회사)는 Context Systems회사와 공동개발에 들어 갔다. Context Systems회사는 ATM운영체계에 중첩하여 쓸수 있는 생체계측대면부용PKI지원응용프로그람들과 망안전관련체계를 제공하는 회사이다. 이 대면부를 리용하면 현재의 표준인 PIN(개인식별번호)을 쓰지 않고도 권한부여와 인증을 할수 있을것이다. 은행에서 쓰는 예금카드에는 지문과 함께 접근카드번호와 같은 고유식별자번호(UIN), 은행구좌번호 등 은행기관들이 사용하는 중요정보를 담게 된다.

개 인 인 증

개인인증은 개인용콤퓨터, 암호작성 및 해독, 자동차 등에 응용할수 있다. 개인용콤퓨터사용에서 인증체계를 응용하는것은 현재 상당히 보급되여 있는 반면에 암호작성 및 해독에는 콤퓨터리용과 함께 가능한껏 응용되고 있다. 자동차에 인증체계를 응용하는 문제는 수감부가 불리한 환경인자들을 이겨 낼수 있는 더 좋은 방도들을 찾아 내면 십분 가능하다.

개인용콤퓨터작업에 개인인증이 제일 먼저 광범히 응용되였다. 무릎형콤퓨터에는 지문수감부가 있어 회사망접속을 위한 인증을 해준다. 수감부의 인증을 받아 해당 쏘프트웨어로 접속개시, 화면보호기, 시동, 파일암호작성 그리고 망접속까지 할수 있게 된다.

Veridicom회사는 무릎형콤퓨터와 기타 휴대형콤퓨터사용자들이 쓸수 있는 지문수감부가 달린 스마트카드읽기장치를 출품하고 있다. 그 목적은 자료접근, 콤퓨터체계, 수자식인증서에 쓰는 통과암호를 다 없애자는것이다. 콤퓨터건반이나 노트형콤퓨터, 무선전화, 인터네트관련장치들에 내장할수 있는 보다 작고 보다 효과적인 인증용수감부도 회사에서 제공하고 있다.

암호작성 및 해독은 무릎형콤퓨터사용자들이 많이 관심을 가지는데 소유자의 지문을 거쳐야만 비밀열쇠를 가지게 되는 잠금통은 매우 주목을 끈다. 콤퓨터소유자는 이 잠금

통을 리용하여 개별망과 인터네트로 정보를 암호화하여 보낼수 있다. 이 잠금통에도 수자식인증서들이나 보다 안전한 통과암호가 있다.

제작업체들에서는 자동차 특히 승용차에 수감부를 설치하고 있는데 차문을 여는데는 승용차문손잡이나 열쇠구멍에 있는 수감판을, 시동하는데는 계기판우에 있는 수감판을 리용하게 되여 있다. 이 업체들은 엄혹한 기후조건이나 내부의 고온상태에서도 정확히 동작할수 있는 능력 등 수감부소편의 신뢰도향상에 주력하고 있다. 연구중에 있는 또 하나의 문제는 높은 준위의 정전기방출을 이겨 내는 능력이다.

기타 새로운것들

기타 새로운 문제들에는 려행자지문적용, 공공신분증카드, 공안감시체계 등이 있다. 려행자지문적용이라는것은 여러 곳을 비행기편이나 철도, 배편으로 자주 다니는 사람들이 비행장이나 국경에서 지문체계에 참가하게 하는것을 말한다. 이런 려행자들은 지문표본하나를 가지고 편리하게 비행기표도 사고 호텔에서 지불도 간단히 할수 있을것이다. 공공신분증카드는 여러 목적에 리용될수 있는데 여기에는 생체계측학적지표들을 다 넣는다. 공안감시카메라체계는 자동적으로 얼굴인식프로그람의 도움으로 밤낮없이 범죄자추적도 할수 있을것이다.

연구자들은 현재 쓰고 있는 얼굴인식알고리듬의 일부 제한요소들을 완화시켜 조명도, 로화, 심부회전과 얼굴표정으로 인하여 생기는 변화값들에 보다 더잘 적응해 나가고 있다. 또한 이미 부분적인 해결을 본 문제이지만 수염, 안경, 화장 등에 의한 모습변화에도 대처해 나갈 방도를 탐구하고 있다.

마이크로쏘프트회사의 노력

2000년 5월 5일 마이크로쏘프트사는 I/O Software사와 합작하여 윈도우즈조작체계에 생체계측인증기술을 결합시키는 작업에 착수하였다. 마이크로쏘프트사는 I/O Software의 생체계측API(BAPL)기술과 SecureSuite사의 핵심적인 인증기술을 얻어 콤퓨터사용자들에게 개인인증방법에 기초한 높은 수준의 망보안체계를 제공하려고 한다.

이러한 기술의 결합으로 사용자들은 자기 콤퓨터에 접속한 다음에는 통과암호대신 지문, 홍채형태나 음성인식과 암호화된 비밀열쇠를 배합리용하여 전자상업거래를 안전하게 진행하게 될것이다. 생체계측모형을 하나 복제하거나 모방하는것은 보다 어렵다. 그것은 두 인물이 가지고 있는 특징전부가 같을수 없기때문이다. 생체계측학적수법이 통과암호나 스마트카드, 개인식별번호를 대처하는데 아주 좋다는 점은 생체계측학적자료들이 망각, 분실, 도난 및 공유의 위험이 없기때문이다.

표 준 화 문 제

생체인식체계와 관련된 산업은 150개이상의 각이한 하드웨어 및 쏘프트웨어업체들을 망라하고 있으며 이 업체들은 제마끔 자기전용대면부와 알고리듬, 자료구조를 가지고 있다. 현재 공통의 쏘프트웨어대면부를 제공하고 생체계측모형을 공유하며 결국에는 서로 다른 생체계측기술을 원만히 비교평가할수 있게끔 표준화하기 위한 사업이 진척되고 있다.

그 한 실례로 BioAPI표준을 들수 있는데 여기서는 임의의 생체계측적응용에도 대면할수 있는 공통의 방법을 규제하고 있다. BioAPI는 60여개의 업체와 정부기관들의 공동투자로 개발된 열린체계의 표준이다. C언어로 짠 이 표준은 사용자이름등록, 신원확인(인증) 그리고 신원발견 등과 같은 모든 생체계측기술들에 공통적으로 존재하는 명령들을 수행하는 기능호출을 다 포괄하고 있다.

BioAPI공동개발국제팀의 초창자인 마이크로쏘프트는 중도에서 떨어 져 나와 자기고유의 BAPI생체계측대면부표준을 개발하였다. 이 표준은 I/O Software사에서 마이크로쏘프트사가 구입했던 BAPI기술에 기초한것이다. 다른 하나의 잠정적인 표준은 각이한 생체계측설비들에서 수집한 모형(templates)들을 교환하고 보관할수 있는 공통적인 수단을 규정한 《생체계측교환파일공통형식》이라는 표준이다. 이 생체인식체계국제개발팀은 또 《공통지문세밀선교환》형식에 대해서도 제안하였는데 여기서는 지문기술관련업체들을 위한 일정한 정도의 운용호환성(interoperability)을 제공하자는것이 목적이다.

운용호환성문제외에 생체계측표준문제는 생체계측적담보 및 시험을 위한 방법론적기초를 마련하는 수단이라고 볼수 있다. 생체계측적담보란 생체계측기구나 설비가 목적한 수준의 안전성을 가지고 있다는 확신을 의미한다. 현재 생체계측지표들을 비교해 볼수 있는 계측지표들은 제한되여 있다.

부분적인 해결책으로 미국방성 생체계측관리실과 기타 그룹들은 현재 표준적인 시험방법론들을 개발하고 있는중이다. 이 사업은 대부분 《공통기준안》의 틀거리안에서 진행하고 있다. 이 기준안은 모든 보안관련제품들의 성능평가와 비교를 표준화하기 위하여 국제적으로 보안관계기관들이 공동으로 개발한 모형이다.

선 택 기 준

정적, 동적 및 결합적인 생태인식체계를 선택하자면 사용자의 실지 감각적인 체험자료, 다른 체계나 자료기지와의 대면부설정의 필요성, 환경조건 등 매 요인들의 특성에 의존하여야 한다.

- 사용상 편리
- 오유빈도
- 정확도
- 원가

- 사용자인기
- 보안요구수준
- 장기적인 적응성

오유빈도를 제외한 이상의 요소들의 등급은 《중》으로부터 《매우 높음》으로까지 매길수 있다. 오유빈도항목은 오유발생원인(례하면 머리타박, 로화, 안경 등)에 대한 간단한 묘사를 념두에 둔다. 여기에는 또한 사기군이 《정확한 본인》으로 인증될수도 있는(다시 말하여 합법적인 본인이 접근배제 당하는 허위배제에 대칭되는 허위접수) 가능성도 포함된다.

결 론

우리는 생체인식기술의 시대로 들어 서고 있다. 한때 연구계획용이라고 하던 많은 새 기술들이 지금은 시장에서 실현되고 있다. 이 기술이 인기를 모으고 있는것은 바로 생체인식기술이 통과암호에 비하여 도난 당하거나 망각되거나 소실될 가능성이 거의 없기때문이다. 그러나 매 생체인식체계는 다 자체의 결점을 가지고 있어 모든 사람에게 다 잘 맞지 않을수도 있고 또 모습이 상당히 달라 지는 사람들에게는 적용되지 못할수도 있을것이다.

얼굴인식, 음성인식, 입술놀림인식기술의 일체화는 흥미 있는 문제이지만 여기서 입술운동의 고세밀도를 보장하는 문제가 더욱 중요하다. 음성을 듣지 못하는 상태에서 입술운동을 읽어 낸다는것이 얼마나 혼돈을 가져 오는가 하는데 대해서는 어떤 사람들은 잘 모르고 있다. 사실상 두세개의 다른 단어를 같은 입술움직임으로 보고 오독하는 경우도 있다. 한때 과학환상소설이나 영화에만 나오던 착용형생체인식체계는 현실로 펼쳐 졌다. 수십년전까지만 해도 만화책에서나 보던 그것들이 지금 군사부문이나 보건부문에서 사용되고 있는 수준이다.

또한 오늘은 무릎형콤퓨터에 비밀열쇠, 수자식인증서, 안전한 통과암호를 담은 지문안전잠금통을 같이 사용하고 있지만 래일에는 승용차의 문손잡이에 손가락끝만 살짝 대도 문이 절컥 열릴것이다. 그러나 이것은 자동차제조업자들이 혹심한 기후조건에도 견딜수 있는 수감소편을 구입하기 위하여 노력하지 않으면 불가능할것이다.

이 모든것들은 표준화문제를 제기하고 있다. 운용호환성과 관련하여 여러 표준안들이 제기되여 몇건이 실행되고 있다. 그뒤를 따라 성능시험방법과 관련한 표준안들이 현재 연구단계에 있다. 표준화사업이 보다 성숙되면 우리가 지금껏 보지 못했던 새로운 생체계측기술들이 시장에 큼직큼직 발을 들여 놓을것이다. 이런 많은 기술들은 동적으로 실시간처리를 할것이며 동시에 보다 상당히 완화된 환경에서 운용할수 있을것이다.

생체인식기술이 이룩하고 있는 진보에도 불구하고 통과암호는 유전적기형, 질병, 년로나 상처로 하여 계측모형을 얻어 내기 힘든 일부 사람들을 위하여 계속 봉사할것으로 전망된다. 물론 이것은 오늘에는 가설에 지나지 않는다. 래일에 특히 아직 설계도에도 없는 획기적인 기술로 하여 래일에는 그렇지 않을수도 있을것이다.

제2장. 보건산업에서의 사적비밀

케이트 보튼

나의 직업적활동안팎에서 혹은 사람들과의 일상 교제에서 내가 알게 되는 모든것, 그러나 밖에 알려 지지 말아야 하는것은 비밀을 지킬것이며 절대로 루설하지 않겠노라

—《히포크라테스선서》중에서—

《의학의 아버지》히포크라테스, BC 약 400년

오래전에 의사들은 단독으로 혹은 조수없이 일하였으므로 환자의 병력을 자기 손으로 직접 썼다. 사사롭고 너무 상세한 자료는 때로 기록하지 않기도 하였다. 의사들은 자기 환자들을 친구나 이웃처럼 알고 있었고 많은 세부들도 알게 되였다. 환자들은 의사에게 직접 현금으로 혹은 물건으로 때로는 봉사로 치료비를 지불하였다. 중간다리는 없었다. 그래서 히포크라테스의 선서는 환자들에게 있어서 귀중한것이였다.

그러나 보건분야의 송달 및 지불체계가 나라의 가장 큰 산업의 하나로 된 오늘에 이르는 과정에 많은 중간매개자들이 생겨 났으며 다량처리과정과 콤퓨터가 펜, 종이, 열쇠 채운 책상서랍을 대신하게 되였다.

결국 의료봉사의 송달과 그에 대한 지불에 너무나도 많은 관계자들이 모두 복잡한 조건과 형식에 따라 끼여 들게 되여 매우 작은 기관들을 제외하고는 모두가 일정한 수준의 사무자동화가 없이는 업무를 볼수 없게 되였다. 다음의 씨나리오에서 자료의 흐름과정을 생각해 보자.

한 사람이 건강보험에 들었는데 그 사람이 호흡기계통에 병이 생겼다. 환자가 진료의사에게 병을 보이니 엑스선흉부투시를 권고한다. 그래서 가까운 병원에 있는 렌트겐과를 찾아 가 투시를 한다. 만사가 순조롭게 되면 렌트겐투시결과가 진료의사에게 전송되며 그 의사는 협의진단끝에 처방전을 써서 약국에 보낸다. 값을 매번 치를수도 있지만 그 엄청난 의료비가 자기의 보험에서 자동적으로 지불될수도 있는것이다. 얼마 지나 《급부금설명서》를 받아 보니 거기에는 의료봉사 받은 내용이 적혀 있는데 그에 대한 비용은 각각 얼마이며 보험에서는 얼마를 지불하였다는것이다. 그러나 그에 대하여 회답을 보낼 필요가 없으므로 아무런 생각도 없이 그것을 어디에 끼워 놓든지 혹은 집어 버릴수도 있다.

환자가 의료봉사를 받고 치료비를 직접 지불하는 과정처럼 매 봉사제공자(진료의사, 렌트겐의사, 약제사 등)와 환자사이의 호상관계가 독립적이며 제한적인것이 못되고 최근에는 치료관계업무들이 막후에서 복잡하게 얽혀 돌아 가면서 환자정보가 멀리에 널리 퍼지게 되는 결과를 초래하는 경우가 많아 졌다.

보건체계내의 몇가지 호상관계만 보아도 환자정보를 어떤 사람들이 알게 되는가를 쉽게 알수 있다.

- 진료소의사
- 진료소의사의 조수들
  - 환자를 접수하고 환자가 병 보이고 갈 때 다음번의 약속을 기록한 의사의 서기나 접수담당자는 흉부투시를 약속한 내용까지 기록할수 있다.
  - 환자의 혈압과 기타 진찰사항들을 환자병력서에 적은 간호원
  - 환자병력서를 꺼내여 의사와 다음 치료시간을 확인하고 다시 서류철에 넣는 병력서담당인원들
  - 인구분포별 및 보험별로 환자들의 림상정보를 편성하여 환자가 치료 받으러 갈 때마다 료금서를 보험계획에 제출케 하는 료금계산원
- 렌트겐의사
- 렌트겐의사의 조수들
  - 환자를 접수한 서기나 접수원
  - 렌트겐투시를 실행하는 기술자
  - 환자의 병력서작성을 담당한 필림담당자들
  - 인구분포별 및 보험별로 환자들의 림상정보를 편성하여 환자의 렌트겐투시후 료금서를 작성하는 료금계산원
- 렌트겐의사가 일하는 병원
  - 렌트겐투시할 때 사용자병원설비의 사용비를 보험에서 받기 위해 문건을 작성하는 료금계산원을 포함한 업무일군들
  - 만일 진료의사가 이 병원의 성원이라면 또한 이 병원에서 그 환자의 병력서를 보관하고 있는 경우 추가병력서담당일군들
- 약국
  - 환자의 이름, 의사의 정보 및 처방과 관련한 사항을 다루는 서기
  - 처방에 필요한 약을 해당 항목에 적어 넣는 약제사
  - 처방을 찾는 환자와 접촉하는 사무원
  - 치료비를 받기 위해 보험자에게 환자정보를 제출하는 료금계산인원
- 환자의 보험회사
  - 진료의사, 렌트겐의사, 병원, 약국에서 각각 들어 온 청구서를 처리하는 청구서처리인원들
  - 하나이상의 보험에 가입하였다면 때로 료금청구서가 다른 보험회사나 보험지사에도 가닿는다.

이렇게 많은 사람들이 자기의 신상정보를 알고 있어 불안하기 시작하였는데 주민분포별 정보, 보험정보, 진단정보, 림상검사정보, 투약정보 등을 포함한 자기의 개인정보를 쉽게 접할수 있는 아래의 보충적인 사람들을 생각한다면…

- 대체로 병원에서 일하면서 정기적으로 기록을 후열하는 품질보증인원들
- 병원설립을 허가한 국가기관이나 조직에서 병원에 대한 검열차로 내려 와 환자의 병력들을 읽어 볼수 있는 검열원들

- 자금모집일군들
- 의사, 병원, 약국과는 별도의 판매담당자들 및 판매회사들
- 연구사업상 목적으로 환자의 상세한 병력정보를 리용할수 있는 연구사들

이제는 그 환자의 상태가 악화되여 병원에 입원하였다고 보자. 환자정보를 아는 사람들의 수는 요란하게 많아 진다.

- 입원접수과인원들
- 식당인원들
- 간병원들
- 병원의 모든 내과의사들
- 의대실습생들, 간호실습생들
- 약국성원들과 약학과실습생들
- 사회사업일군들과 학생들
- 환자입원내용을 전부 병원으로부터 보고 받는 국가기관들

마지막으로 다른 하나의 껍질을 벗겨 보면 더 나온다.

- 보건관계자료기지, 봉사기, 망을 관리하는 여러 정보체계운영자들
- 고객지원체계를 제공하는 여러 콤퓨터체계판매자들
- 제3자업무일군들 례하면
  - 환자에 대한 의사의 기록을 옮겨 적어 열쇠 채워 보관하는 필사원들
  - 병원의 전자자료를 변환하여 보험회사에서 받아 볼수 있는 형태로 만드는 자료쎈터들
  - 법률회사들
  - 재정검사일군들

그 환자가 단순한 호흡기질환이 있는것이 아니라 HIV(인간면역결핍비루스)감염이 와서 앓는것이라면 어떻게 될것인가. 워싱톤시종합병원의 경우를 보자. 한 병원직원이 비밀을 지키지 못하여 한 환자의 HIV상태에 관한 내용이 환자의 동료들에게 새여 퍼졌다. 재판소는 이 병원이 환자에게 25만딸라의 보상을 낼것을 판결하였다.

많은 사람들은 자기들이 가지고 있는 기록들에는 기밀적이거나 공개되면 혼란이 일어 나거나 차별대우를 초래할만한것이 없다고 하지만 그래도 거기에는 기초적으로 보호되여 기밀취급되거나 접근조종을 해야 할것도 있다. 결국 이것들은 다 정보보안의 기초틀거리에 속하는것이다.

개인들의 건강정보가 어떻게 리용되며 퍼지는가 하는데 대해서 알게 되는 경우는 매우 드물며 일부 사람들에게 례외적으로 특정정보를 제한하는 특권을 주는 경우는 더욱 드물다.

이러한 정보공유는 사실상 대부분 합법적이거나 필수적이기도 하다. 치료를 잘 받으

려면 해당 정보전체에 대한 치료관계자들의 접근이 허용되여야 한다. 치료비청구서를 받아 지불하기 위해서도 보험회사가 환자정보를 알아야 한다는것은 누구나 다 인정한다. 그러나 보건산업이 그 문을 활짝 열어 놓음으로 하여 은연중 첫째로는 필요이상의 많은 인원들이, 둘째로는 필요이상의 많은 정보에 불필요하게 접근하게 되는것이다. 그리하여 특전의 최소화라는 기밀정보보안원리가 위반되고 있다. 치료일군들은 알아야 하지만 그 병원의 모든 치료일군들이 다 알 필요는 없을것이다. 보험회사들이 필요한 정보를 알아서 청구된 지불액이 합당하다는것을 확인할 필요가 있다는데 대해서는 리해되지만 오늘날처럼 그렇게 상세한 개인정보를 꼭 알아야 할 필요가 있겠는가 하는것은 명백치 않다.

최근까지만 해도 전반적인 보건산업에 공식적인 정보보안계획이 부족하였다. 여러가지 리유가 있다. 하나는 대량적으로 생기는 의료관계자료들이 상업적가치가 별로 없으므로 의료기관들이 정보도난대상으로 될것 같지 않다는 견해이다. 개인병력들이 외부에 왕왕 류실되는 경우들은 있었지만 보건부문에서는 이것들을 례외적인것으로 보았다. 유명한 정구선수 아써 애쉬는 자기가 HIV양성반응이라는 실태를 비밀에 붙이기 위해 온갖 고생을 하였지만 한 의료일군이 보도계에 그것을 루설하고 말았다. 개인들의 사적비밀이 침해되는 실례는 자주 일어 나지만 밝혀 지지 않을뿐아니라 환자에게 뚜렷한 그 어떤 손해도 주지 않는것은 사실이다. 이제 와서야 사람들은 약상점들이 제약회사들과 환자처방기록들을 함께 가진다는것을 알고는 놀라서 일반사람들의 의료기록을 담는 대용량자료기지에 상업적가치가 충분히 있다고 보기 시작하는것 같다.

병원을 비롯한 보건기관들은 전통적으로 륜리와 명예라는 일차적인 가치체계는 세워놓았지만 일관성 있고 구체성 있으며 규약으로 밝혀 진 기술적인 통제는 실시하지 못하였다. 결국 모든 의사들(덧붙여 보면 의사의 조수들까지 포함하여)은 륜리를 잘 지킨다, 환자가 앓아 위기에 처할 때 환자정보를 누구도 막으려 하지 않는다는 체념이 존속되여왔다. 불행하게도 이러한 관점은 잘 맞지 않는다. 매 사람의 행동을 한 눈으로 볼수 있는 자그마한 사무실에서는 몇가지 절차와 기술적통제만 덧붙이면 충분할지 모르나 보건기관이 커지고 기능이 많아 지게 된 조건에서 이런 관점만 가지고는 환자정보의 비밀성, 무결성, 사용성이 담보될수 없는것이다.

치료와 치료비지불에서 공식적인 건강정보보안질서의 부족으로 사람들이 불안해 하는데 다른 편에서의 개인정보의 2차적인 사용은 우리가 전혀 알지도 통제하지도 못하고 있는 형편이다.

《자료기지의 나라와 21세기 개인성의 사멸》이라는 책에서 씸슨 가핑켈이 신랄히 주장하듯이 우리 매 사람에 대해서 그렇게 많은 정보가 수집되고 우리가 상상 못할 정도로 그렇게 많은 분야에서 그것이 리용되여 본적은 일찌기 없었다. 신원도난은 급격히 성하는 범죄현상이다. 이 장에서는 언급되지 않지만 이 범죄현상에 대해서는 여러 곳에서 자료를 얻을수 있다(법무부 Web싸이트 www.usdoj.gov나 사회보장국의 Web싸이트 www.ssa.gov 등에서 신원도난문제를 보라.). 매일매일 일어 나는 사건과 사변들 그리고 그 파괴적후과에 대하여 다 명백히 알지는 못하지만 지금 어딘가에서는 사람들의 사적비밀이 매우 위험한 수준에서 위협 받고 있다는 의식은 상당히 높아 지고 있다.

1999년 9월 월스트리트저널과 ABC방송사가 공동으로 21세기의 가장 큰 불안감이 무엇인가에 대하여 여론조사를 해보았다. 경제적, 정치적 및 환경적불안감이 먼저 떠오를

것 같지만 가장 많은 응답이 인간의 사적비밀상실이라고 하였다.

보건분야에서는 이것이 무엇을 의미하는가. 이 우려가 우연치 않다는것을 보여 주는 실례는 허다하다.

- 의사의 정상검진을 받은후 플로리다주 오를란더우에 사는 한 녀성은 제약회사로부터 고콜레스테롤치료약을 소개하는 편지를 받았다(《오를란더우쎈티널》잡지에 게재된 기사《의사에게 하는 말을 많은 사람들이 듣는다. 환자기록의 비밀이 보장 못되여) 1997년 11월 30일 A1페지).
- 지방 보건리사회에서 일하는 한 은행업자는 환자정보를 입수하여 자기 은행의 대부정보와 비교해 보았다(《전국법률학보》 1994년 5월 30일).
- 한 정신병치료전문가에 대한 협잡건을 수사하던 과정에 련방수사국은 환자들에 대한 병력을 입수하게 되였다. 환자들중에서 자기네 련방수사국 직원 한명을 발견한후 근무비적합으로 보고 압력을 가해 조기은퇴하게 하였다. 후에 그는 근무적합으로 밝혀 졌다. (《로스안젤스 타임스》기사《의사만 보는 병력서가 이젠 아니다)1998년 9월 1일 A1페지)

이러한 현실은 보건분야에 부정적그늘을 던져 주고 있다. 한 의학자협회의 평의회 성원인 도날드 파미싸노박사는 《만일 환자가 자기 병력정보의 비밀이 보장된다고 믿지 않으면 우리는 그에게서 진단에 필요한 정보를 얻지 못할것이다.》라고 말하였다(《보스턴 글로브 매거진)2000년 9월 17일 7페지).

1999년 1월 프린씨턴조사연구집단이 캘리포니아보건재단이 의뢰한 조사를 벌리고 《미국성인의 15%가 자기 개인병력정보의 비밀을 지키기 위해 비정상적인 거짓말을 하였다. 자기 비밀을 지키기 위한 방도에는 자기의 건강을 크게 모험하는 행위들도 있었다. 환자들은 지어 다른 의사들에게 찾아 가는것, 기업주에게 알려 질가봐 아예 치료를 받으려고 하지 않는것, 기왕력을 부정확하게 혹은 불완전하게 말하는것, 의사에게 병명을 병력서에 쓰지 말라고 부탁하거나 경감해서 약한 병상태에 있는것으로 기재할것을 부탁하는것 등이 그들이 쓰는 수법들이다.》라고 밝혔다.

보건분야에서 사적비밀과 신용이 부족한 현상은 법률을 통하여 마침내 가까스로 시정되고 있다.

HIPAA

1996년에 채택된 《보건보험공용 및 책임관계법》(HIPAA)에는 여러가지 목적이 있는데 그중 하나는 보건체계에서 업무기관들사이에 진행하는 전자거래의 표준화를 추진하여 원가를 절약하자는것이다. 그리하여 이 법이 실시되면 개별적사람이 보험계획에 드는 경우와 치료비청구와 지불이 있게 되는 의료봉사를 받는 경우에 기업주, 제공자, 지불자들의 공통의 고유식별자들과 표준코드를 리용하여 표준화된 형식의 전자기록으로 해당

정보들이 교환된다.

표준화가 원가를 떨구지만 정보보안과 사적비밀보장에는 위협이 커진다는 사실을 국회가 다행스럽게 인식하였다. 예전에 없이 개인건강정보들이 전자형태나 보통형식으로 만들어 지고 있는 조건에서 임의의 사람이 우리의 정보를 불법입수하여 리용하기가 더 쉬워 졌다. HIPAA는 개별적인 형식화를 청산하였으므로 모든 사람들은 《불투명에 의한 보안》이라는 안전성의 일부를 잃게 된다. 자기 의사가 자기 건강정보를 알게 하는것이 직접적인 도움을 주지만 이 정보가 자기 기업주와 판매회사에 알려 지면 상당히 대가가 크던지 아니면 곤경에 빠지게 된다.

그리하여 국회는 이 법에 보안과 사적비밀보장에 관한 요구사항들을 첨부하였다. 이 법은 보건성에 정보보안시행세칙을 작성할것을 위임하였으며 그렇지 않으면 보건성이 개입하여 사적비밀보장시행세칙을 작성하게 되여 있다. 수많은 보건사적비밀보호안들이 위원회에서 토론되였지만 국회표결단계까지 오른것은 하나도 없다. 결국 보안시행세칙과 함께 사적비밀보호세칙도 보건성이 떠맡게 되였다. 그러나 보건성도 권한이 제한되여 있는것만큼 자료변환기관과 법률상담회사 등 보건정보를 사용하는 많은 주요기관들은 자기의 권한행사권밖이므로 빼놓고 다만 보건봉사제공기관들과 건강보험회사들만 규제할수 있는것이다. 그러므로 국회에서 포괄적인 건강사적비밀보호법을 통과시키기전까지는 우리의 법률적보호장치에 큰 구멍이 나 있는셈이다.

HIPAA의 사적비밀보호사항은 2000년 12월에 완료되였으며 모든 관계기관들은 이 사항을 2003년 2월까지 준수하게 되여 있다. 이 글을 출판하는 순간까지 HIPAA에는 정보보안사항이 제안의 형식을 띠고 아퀴를 짓지 못한 상태로 있다.

정보보안과 사적비밀규정세칙들은 서로 어떤 관계에 있는가. 정보보안전문가들은 일반적으로 정보보안이란 보호되여 있는 정보의 비밀성, 무결성, 사용성을 담보하는것이라고 정의하고 있다. 보건분야에서 비밀성이 가장 큰 관심을 끄는 리유는 바로 환자정보가 감정적으로 매우 예민한 문제이기때문이다. HIPAA보안사항의 작성자들은 전반적범위의 보안을 고려하여 전반적인 정보보안계획을 요구하였다. 결국 례를 들어 보면 실험검사소견의 무결성과 알레르기반응소견의 사용성문제가 그 사람의 건강에 결정적으로 중요하게 되였다는것이 아닌가!

이로부터 HIPAA의 규제하에 들어 가는 모든 기관들이 공식적인 정보보안계획을 실행해야 할 책임을 지고 있는셈이다. 다른 한편으로 본다면 사적비밀보호개념의 중요한 초점은 개인에 귀착된다. 사적비밀보장법들은 개인정보접근과 통제와 관련하여 매 개인이 가지는 권리를 명시하며 이러한 권리를 보장하기 위하여 관계기관들이 준수해야 할 의무를 규제하는것이다. 사적비밀보장은 정보보안을 필요로 하므로 많은 점에서 이것은 한 동전의 량면인셈이다.

적절하고도 설득력 있는 보건사적비밀보호법초안작성에서의 난점을 예상하여 국회는 보건장관에게 권고안을 제출할것을 요구하였다. 당시 보건장관이였던 도너 샬랄라는 1997년에 다섯가지 원칙에 기초한 보고서를 제출하였다. 이 다섯가지 원칙은 수십년전에 정부가 이미 작성한 《공명정보관례》에 준한것이다.

이 공명정보관례들은 《공정한 신용보고법》의 기초로 리용되였다. 이 법은 사람들에게 자기들의 재정신용보고서를 은행기관들에서 거의 비용없이 평문으로 한부 구입하거

나 오유들을 솔직하게 수정 받을 권리를 주고 있다. 이 공명정보관례는 유럽과 일련의 많은 나라들에서 사적비밀보장의 법적토대로 되고 있다. 그러나 미국에서는 사람들의 개인정보에 대하여 지나친 통제를 하는 정부의 위구심으로 하여 전면적이며 련방적인 사적비밀보장법의 채택운동이 1970년대에 무산되고 말았다.

샬랄라의 5가지 원칙은 다음과 같다.

- **경계선** 어느 한 목적을 위해 수집된 정보는 본인의 긴급동의가 없는 한 다른 목적에 사용될수 없다.
- **소비자의 통제** 개인은 자기에 대한 기록자료를 한부 가질 권리, 그 기록에서 틀린 점을 수정할수 있는 권리, 그 정보가 현재 어떻게 리용되고 있으며 그것을 어느 기관들에 주었는가를 알 권리를 가진다.
- **사회적의무** 개인의 권리와 사회의 리익사이에는 공정한 균형이 있어야 한다(다른 말로 말하면 사적비밀에 대한 권리에는 절대성이 없다.).
- **책임소재** 이 규정들을 어길 경우 책임 있는자들은 법적제재를 받는다.
- **안전보호** 각 기관들은 개인자료로 판명되는 정보들을 책임지고 통제하고 보호할 의무를 진다.

마지막원칙은 HIPAA의 보안요구사항과 사적비밀요구사항들사이의 관계를 리해하는데서 특별히 중요하다. 이것은 접근조종분야 같은데서 보안이 없는 비밀이란 생각할수 없다는것을 명백히 보여 준다. 보건성이 제안한 HIPAA의 사적비밀보호조항은 개인의 건강정보에로의 접근이 어느 경우에 적합하며 어느 경우에 부당하며 또 어느 경우에 명백한 동의가 필요한가 등을 밝히고 있다. 또한 《필요의 최소화》보안원리의 준수, 재정검열흔적의 창조, 종업원들에 대한 보안강습 등을 요구하고 있다. 이 규정들을 그대로 적용하면 상용보안 및 접근조종장치로 되여 기관의 공식적인 보안계획 즉 보안방책, 보안절차, 물리적 및 기술적보안통제, 보안교육 등을 세워 놓을수 있다. 실지 사적비밀보호조항은 넓은 의미에서 보면 안전담보장치의 필요성을 재확인함으로써 HIPAA에서 달리 취급된 보안조항의 요구들을 다 담고 있는것으로 리해할수 있다.

환자의 사적비밀보호와 관련한 기타 법률

1999년에 대통령은 일부 마음에 들지 않는 부분이 있었지만 《그램-리치-블릴리법》(GLB)에 서명하였다. 이 법에 의하여 보험, 은행, 중개업들사이의 법적장벽이 다 무너짐으로써 이 분야들사이에 정보를 통합 및 공유할수 있게 되였다. 이것으로 하여 풍부한 시장호기가 있을것이라고 하지만 그러나 이 GLB의 사적비밀보호사항에도 불구하고 개인들은 자기들의 상세한 사적인 정보와 지어 건강정보의 공유에 대하여 통제권을 얼마 가지지 못할것이다. 대통령이 개인들에게 보다 큰 통제권을 주겠다고 공약하였으나 HIPAA 사적비밀조항에 의하여 건강자료에 대해서는 얼마나 통제권을 가지게 되겠는지.

1995년 엘렌 앨더맨과 캐롤린 케네디 두 변호사가 쓴 《사적비밀보호의 권리》에서 보여 주듯이 전국적으로 볼 때 사례적인 법률 및 사적비밀보호문제에서의 결과들은 일관하지 않다. 그러나 1991년부터 시작된 프린씨턴보건쎈터와 HIV(인간면역결핍비루스)양성으로 나타난 그곳 한 의사를 둘러 싼 사건이 던져 주는 의미는 크다. 법정에서는 그 의사에 대한 치료의무가 없음에도 불구하고 그의 병력을 조회해 본 쎈터직원들이 그 의사의 사적비밀권을 침해한것으로 판결하였다. 다시 말하여 직무상 《알아야 할 필요성》이외의 목적으로 그의 정보를 뒤져 보았다는것이다. 법정은 이것을 사적비밀에 대한 침해로 규정하였다. 이 사건은 정보보안분야의 일군에게 정보보안의 기본사상을 확증해 준다.

HIPAA가 출현하고 보안과 기술령역에서의 법관들과 변호사들이 점차 정교화됨에 따라 이러한 법적상소건들이 더 많을것으로 생각된다.

새로운 사적비밀보호법과 규정의 준수와 관련한 기술적난점

모든 보건기관들이 HIPAA보안 및 사적비밀보호요구사항들을 세밀히 분석해 본 결과 기술적으로 준수하기 힘든 문제들이 여러 군데에서 나타나고 있다.

세부적접근조종에서의 난관

현재 제기되고 있는 기술적난관의 하나는 허용된 사용자의 접근을 제한하는 응용프로그람에서 충분히 세분화된 조종이 부족한것이다. 이 문제는 여러가지 측면을 담고 있다.

첫째로, 지금까지 오래동안 직무에 기초한 접근조종을 통하여 기능이나 자료형태별로 접근을 통제하는 체계들이 리용되여 왔으므로 어떤 특정한 환자에 대해서만 접근을 제한하는 알고리듬을 개발하기는 힘들다. 례하면 환자주소나 보험계획자료를 기록하거나 시간갱신하자면 환자등록담당자들이 지역별 환자자료와 보험자료를 보아야 하는것이 정상이다. 그러나 환자의 실험소견이나 환자상태에 대한 담당의사의 기록에 대해서는 접근하지 못한다. 다른 한편 환자등록담당자들은 그 병원에 있는 모든 환자들의 지역분포별 및 보험자료들을 다 보게 된다. 그런 정보들이 력사적으로 보관되였기때문에 등록담당자는 그러한 개인정보를 수천건이나 볼수 있게 된다. 그런 정보들은 대개 그리 기밀적인 성격이 없는것으로 본다. 사람들의 이름, 주소, 전화번호들은 전화번호책에도 출판되여 나와 있으며 대부분의 사람들은 자기가 든 보험계획의 이름을 비밀에 붙이지 않고 있다. 그런데 이 정보들은 HIPAA의 완전한 보호밑에 들어 가 있으며 보호하지 않으면 사람들을 위험에 빠뜨릴수 있다. 남편에게 두들겨 맞고 도망쳐 숨어서 치료의 손길을 청하는 녀성이 있다고 보자. 자기에게 와서 치료해 주려는 의사에게 자기 집주소를 기꺼이 보낸다. 그 녀성은 이 정보를 비밀에 붙이고 자기 남편에게 이것이 루설되지 않기를 응당 바란다.

세분적접근조종이 더 곤난한 점은 환자의 실제 의료정보인 진단, 실험결과, 의사소견,

수술 및 기타 절차, 복용한 약명세 등에 대한 넓은 접근에서 볼수 있다. 병원의 모든 의사들과 그 보조성원들이 수천 지어 수백만건에 달하는 환자기록들인 력사적으로 된 자료기지에 접근할수 있는것은 비정상적인것이 아니다. 의대실습생들과 료금계산 및 의료기록과 관계되는 수많은 인원들도 마찬가지이다.

이러한 경우에 의료기관들에서는 위험을 인식하며 모든것이 그 보안체계판매자들에게 달려 있으며 그들의 제품들에 더 엄격한 통제기능이 없어서 그럴수밖에 없다고 말한다. 미흡한 체계의 보안을 위해 일부 기관들에서는 보안방책, 보안공정, 보안강습 등의 보상조치들을 강구하기도 한다. 보건기관들에서 일하는 근무자들에게 직무상 알 필요성이 없으면 정보에 접근하지 않겠다는 기밀보장합의서에 서명시키는것은 보통일로 되고 있다. 많은 기관들은 그것으로 자기 기관이 보건정보비밀성을 지킬 의무를 충분히 수행하고 있는것으로 자기만족에 빠져 있는것이다.

사실 이 문제는 소홀히 대할 문제가 아니다. 자그마한 보건기관이라면 문제가 명백하나 학술적인 의료쎈터, 더 나아가서 가장 복잡한 전문종합병원 같은데서는 많은 성원들중 어느 전문일군들, 어느 보조성원들, 어느 업무 및 행정일군들이 어느 환자의 병력에 접근하였는가를 통제한다는것은 정말 불가능하다.

이러한 현상은 체계전문설계가들로 하여금 흥분되여 창조적인 방안들을 개발하게 하고 있다. 실례로 영국에서 케임브리쥐대학의 로쓰 제이 앤더슨박사가 개발하여 여러 병원들에서 응용되고 있는 새로운 체계는 환자별로 구별되는 접근조종목록(ACL)을 쓰고 있다. 이 ACL은 환자의 담당진료의사가 관리하는데 의사는 실례로 이 목록에 협의진단에 필요한 전문가들의 이름을 림시로 추가하기도 한다. 보조성원들은 해당 담당의사들과 련결시킴으로써 해당한 접근을 가지게 한다.

해당 환자와의 관계에 기초하여 이와 류사한 정황별 접근조종해결방식을 개발할수 있다. 실례로 여러 보건계획들에서는 환자치료사업을 위한 첫 입구문지기로 진료의사를 지정할것을 요구하고 있다. 보건실천에서는 이렇게 진료의사와 협의의사를 지정하거나 혹은 고정할것을 요구하고 있다. 그래서 입원체계에서 입원환자를 제기하는 의사, 입원환자를 받는 의사, 입원환자를 담당할 의사 등을 지정하는 체계가 오랜기간 존속되여 왔다. 그리하여 표준적인 역할별 접근조종외에도 대상환자에 대한 매 의료인원들의 접근을 보다 제한할수 있다. 그러나 해결방안들은 행정적으로 관리하기 쉬워야 하며 정보에 대하여 많이 접근하는 비전문가들에 대해서도 반드시 적용되여야 할것이다.

개략적인 알고리듬이 개발되여 환자전체에 대한 부분적인 세부항목들이 규정되였다 하더라도 《유리창깨기》기법이 쉽게 적용될수 있다. 이 과정을 본다면 다음과 같다. 자기 담당이 아닌 환자에 대한 기록에 의사가 접근할 필요가 있을 때 《이 환자기록을 정말 보시렵니까? 이 접근은 기록되고 검열됩니다.》라는 식의 경고문이 화면에 나오게 할수 있다. 의사가 계속하여 환자기록에 접근하면 경보가 울린다. 가령 경고문이 보안담당자의 휴대형호출기에 보내여 지거나 계속하여 다음날 업무시작전에 검열기록보고서가 화면에 뚜렷이 현시될수도 있다.

이런 장치가 있으면 비법적인 자료열람에 강력한 제동기적역할을 가할수 있을것이다.

세부적접근조종이 안고 있는 두번째 측면은 HIPAA의 사적비밀보호조항의 요구사항에 있다. 이 조항은 의료기관들이 매 환자에게 환자정보를 해당 약구입과 같은 특수한

경우 매번 사용허가를 받을것을 규제하고 있다. 환자들은 동의하였다가 후에 그 허가를 취소하는 때도 있다. 이것은 열람리유가 약구입을 위한 판매관계라면 자료기지접근프로그람이 자료기지에 있는 매 환자의 기록자료에 자유롭게 접근할수 없게 할수도 있다는것을 시사해 준다. 기록자료를 복원하기전에 그 쏘프트웨어는 해당 환자의 명백한 의견을 일정하게나마 확인하지 않으면 안된다. 이것은 기술적으로 볼 때 까다로운 문제가 아니지만 그 접근을 위한 리유를 밝히는 문제는 까다롭다. 흔히 보안체계에 미리 설정해 놓은 사용자의 역할에 기초하여 추측할수도 있을것이다. 실례로 사용자가 약품구입처에 근무하며 그에 따라 허가를 받은 상태라면 그 접근의 목적이 약품구입과 관련된것으로 추측판정할수 있다. 가장 명백한 례는 환자관리를 1차적인 역할로 하는 내과의사의 경우이지만 그가 행정 및 연구사업에 관여할수도 있는것이다. 일부 프로그람제작 및 판매업체에서는 이 문제를 해결하기 위하여 자료에 접근할 때 접근자에게 여러 항목중에서 접근리유를 찍어 선택할것을 요구하는 수법도 써보았다. 그러나 정보보안전문가나 검열자들의 눈에는 접근리유를 접근자자체가 선택하는것이 보안통제로 보일리 만무하다.

환자준위의 후열

우에서 본바와 같이 충분한 정도의 세부적접근조종이 부족한데다가 사람들이 가지고 있는 호기심이라는 경향까지 겹쳐 사업상 허가를 받은 리유이외에도 많은 사람들이 비법적으로 환자정보를 여기저기 뒤져 보거나 찾아 보는 현상이 매일 벌어 지고 있다. 가장 좋게 보면 이것을 자기 가족, 친척, 친우, 동료에 대한 동정이나 우려때문이라고 할수도 있다. 가장 나쁘게 보면 이것을 나쁜 목적이나 금전상의 리익을 노린것으로 볼수도 있다. 《국민의료보장제도》(65세미만의 저소득자나 신체장애자를 위한다는 보건제도-역주)의 한 직원집단은 대상환자들의 재정원천에 대한 자료를 복사하여 산하 의료기관에 팔아 먹은것으로 하여 기소되였다(잡지《포브스》 1996년 5월 20일 252페지).

이러한 행위는 분명히 보건기관들에 맡겨 진 자료의 비밀성 그리고 개별적환자의 사적비밀에 대한 위협으로 된다. 자료를 간단히 읽어 보기만 해도 환자에게 극단한 해를 주게 되는 보건기관인 경우 그 피해는 더없이 크다.

망에서 자료뒤져보기가 비법적으로 너무나 성행한데 우려하여 병원성원들자체가 자기 병원에서 치료받기를 꺼려 하고 있는 실정에서 강력한 대책을 세워야 할 때는 왔다. 수년전에 어느 한 병원에서는 이러한 페단을 막기 위하여 환자들에 의한 후열기능을 자기의 직결구내체계에 추가하였다. 그때로부터 다른 병원들과 일부 보건제품판매업체들이 이 귀중한 정보보안기능들을 자기들의 체계에 적용하기 시작하였다. 이 기능이 표준적인 자료기지후열흔적이나 정보변경기록과 개념상 다른 점은 접근하였던 정보가 변경되였든 변경되지 않았든 관계없이 모든 접근이 전부 기록된다는 점이다. 둘째로 자료기지후열흔적과는 달리 환자자료가 아닌이상 자료열람기록을 정확하게 하는것은 그리 중요하지 않다. 가령 한 사용자가 사업상 리유와는 관계없이 옆사람의 기록을 찾아 본다면 정보가 얼마나 중요한가에는 관계없이 보안규칙은 깨여 진것이나 다름 없다.

무단적인 뒤져보기는 하나의 근본적인 사적비밀침해문제로서 HIPAA에서는 의료기관들에 환자들에 의한 후열흔적과 같은 정보보안기법을 통하여 이 문제를 해결할것을 촉

구하고 있다. 이 후열흔적을 리용하면 허용된것이든 허용되지 않은것이든 자기들의 정보가 어떻게 각이한 리유로 열람되였는가를 환자들에게 요구에 따라 통보해 줄수 있다.

이 형태의 후열흔적에서 기술적문제로 나서는것은 성능과 보관의 영향 그리고 방대한 량의 후열흔적기록을 조사하는것이다. 이 형태의 후열흔적은 실천상 모든 환자들에게 다 해당되여야지 어느 특정한 환자들에게만 해당되여서는 안된다. 그러므로 이 후열흔적기능을 잘 설계하지 않으면 전반 체계성능이 예상외로 떨어 질수 있다는것은 상상하기 어렵지 않다. 류사한 문제로서 매 후열기록용량이 직결보관공간의 견지에서 고려되여야 한다는것이다. 콤퓨터능력과 보관의 가격이 떨어 지는데 따라 이것들은 그리 큰 문제로 되지 않을것이다. 그러나 남은 기술적문제는 방대한 량의 후열용자료들에서 람용건을 분석하고 찾는 도구를 어떻게 만드는가 하는 문제이다. HIPAA의 조항에 의하면 문제가 제기되면 이러한 후열흔적을 가지고 있는것만으로는 안되게 되여 있다. 즉 기관들이 이러한 파일들을 사전행동으로 미리 조사해 보게 되여 있다. 그런데 방대한 량의 적합접근건중에서 비적합접근을 하나 찾아 내는것은 현재 간단한것도 아니며 또 흔히 하는것도 아니다. 적합접근과 비적합접근을 구별해 낼수 있는 령리한 려과장치가 필요한것이다.

인터네트사용

보건산업이 인터네트를 일정하게 놀랄 정도로 광범위하게 받아 들이고 있는것은 새 기술의 초기보급자로서의 명성이 알려 지지 않아서 그것을 회복하느라고 그러는지도 모른다. 어쨌든 인터네트가 한 기관이 여러 지역에 널려 있는 경우에 제공자와 지불자사이, 궁극에는 기업과 소비자사이의 통신수단으로서 매우 유혹적인것만은 사실이다.

오래동안 인정된 사실이지만 통신문이 암호화되고 사용자들에게 강력한 두 요소인증체계만 있으면 인터네트를 상대적으로 마음 놓고 쓸수 있다. 사실 이것들이 보건부문에 대하여 HIPAA가 요구하는 인터네트사용기준들이다.

암호화요구사항을 만족시킬수 있는 오늘날의 제품과 대안들은 수없이 많으며 거기에 쓰이는 공인된 알고리듬들은 3DES, RSA, ECC이며 AES는 가까운 시기에 곧 출현할것이다. 그러나 인증요구사항은 실행상 상당한 난점을 제기하고 있다.

오늘날 많은 보건기관들에서는 개인식별번호(PIN)와 통표를 사용하여 먼 거리에 있는 사용자를 믿음직하게 두 요소로 인증하고 있다. 현재 인터네트기업활동이 얼마나 빨리 확대되고 있는가를 보면 이 인증방식도 보건산업의 소비자들 즉 사회전반에 표준화할수 없다는것이 자명해 진다. 그러나 HIPAA는 보건기관들이 환자나 건강보험가입자와 통신하는 경우 그 보호의무를 소홀히 하는것을 법적으로 허용하지 않고 있다.

인터네트로 환자건강보험의 가입성원들과 서로 망으로 련계를 맺는 보건기관들의 실례는 허다하다. 일부 병원들은 환자들에게 자기 실험결과를 비롯한 치료정보의 열람을 허용하고 있다. 일부 보험계획에서는 가입자들이 자기 주소나 진료의사지정을 갱신하도록 허용하는 체계도 리용하고 있다. 의사나 보험계획과 환자들사이의 전자우편통신은 보편화되고 있다.

텍싸스주 댈러스시에 있는 로스페로트가 경영하는 회사인 페로트 씨스텀즈는 보스턴지역의 주요보건기관인 《하바드필그림보건》과 수백만딸라의 계약을 맺고 《인터네트에

기초한 ＜미래적인 보건기관＞창설》에 착수하였다.

2000년 11월에 첫 단계로서 Web싸이트를 개설하여 종업원들이 보건계획에 가입하도록 하였다. 그러나 앞으로 《페로트는 병원들, 의사들, 기업주들, 성원들 그리고 보건기관 전체가 망에 가입하고 환자정보를 시간별로 갱신할수 있는 체계 즉 <21세기에 실시되여야 할 의학의 본보기>를 내다본다.》(엘 꼬왈스위크의 기사 《페로트의 보건리상:억만장자와 하바드필그림은 인터네트에 기초한 체계를 본다.》《보스턴 글로브》신문 2000년 3월 8일부 D1페지).

그러나 이러한 통신은 흔히(언제나 그런것은 아니지만) 암호화되지만 표준적으로는 환자나 가입자가 정적인 통과암호나 개별식별번호로만 인증하는 방법으로 진행된다. 보건기관들인 경우에 두 요소인증방법을 리용하여 자기 종업원들의 전화망접속을 실현시키는데도 이런 방식을 쓴다.

그렇다면 이렇게 호상 현저히 차이나는 수준의 보안을 어떻게 량립시키는가. 오늘날 많은 보건기관들은 HIPAA요구사항들은 알지도 못하고 있으며 리유를 불문하고 사회와 진행되는 정보통신에는 적용되지 않는것으로 기대하고 있는것이다. 이러한 회피현상은 두요소인증해결책의 실현과 그 해결책을 모든 환자나 보건계획가입자들에게까지 확대하는것이 실지로 비용(딸라나 품)이 많이 들거나 많이 든다고 생각하는데 기인된다. 그런데 보건관련인터네트거래량과 보건업무상 용도가 앞으로 더 확대될것은 분명하다. 그러나 일부 기관들에서는 이러한 보안통제를 자기 기관의 금후 몇년간의 전략적목적의 테두리안에서 어떻게 실현할것인가에 대하여 고려하기 시작한데 불과하다.

가장 가능성 있는 해결책은 현재 공개열쇠기반(PKI)과 수자식인증서 및 서명체계를 실행하는데 있는것으로 보아 진다. 일부 PKI지지자들이 잘못 생각하고 1988년에 제기된 HIPAA보안 및 수자식서명표준안이 PKI채택을 요구할것으로 주장하고 있지만 운용호환성기술들의 집합체인 PKI는(암호화, 부인방지, 통신문의 무결성과 더불어) 강력한 보안통제수단을 포괄하는 강한 원격인증을 위한 확고한 약속을 안겨 주는것이라고 보아 진다.

신용카드와 은행카드가 무형의 형태로 리용될 때 금융세계에서 나타날수 있는 사기협잡의 가능성들에 대하여 생각해 보라. 전체 신용카드거래의 몇프로만 인터네트를 통하여 진행되지만 사기건의 대부분은 바로 신용거래에서 생기고 있다. 또한 Visa USA사에 의하면 《협잡주문건수가 벽돌건물상점에서는 100딸라당 6쎈트밖에 안된다면 인터네트상으로는 100딸라당 10～15쎈트에 이르고 있다.》(《보스턴 글로브지) 2000년 10월 9일 C1, 9페지). 소비자의 책임은 극히 적으며 은행 잘못도 아니다. 1999년에 American Express사는 American Express Bluecard를 도입하였는데 여기에는 바로 신원(카드소지자의 인증)의 확인과 보안을 보다 강화하기 위한 전용소편이 들어 있다. 특히 최근에 VISA사도 소편을 내장한 카드를 공급하기 시작하였다. 두 경우에 카드읽기장치는 소비자들에게 자유판매할수 있다. 사기건의 위협으로 딸라손실을 예상한 많은 기업들이 사기방지대책을 취함에 따라 PKI산업은 추동력을 얻어 표준화, 응용호환화, 보다 눅은 원가에로 점차 나아갈것으로 보인다.

우리가 쓰는 은행카드와 신용카드가 수자식인증서를 내장한 스마트카드로 되면 가정용콤퓨터나 무릎형콤퓨터에 인차 스마트카드읽기장치를 가지게 되는것이 표준으로 될것이며 이 카드읽기장치들은 여러가지 카드를 다루게 될것이다. 처음에는 이것이 수십년전

에 그러하였던것처럼 연유공급소와 백화점에서 받은 신용카드가 가득 찬 돈지갑과 류사한 새 세기판 돈지갑으로 볼수 있을것이다. 많은 기업들과 기관들이 서로 자기의 스마트카드를 발급하고 그것을 통하여 그 카드의 소유자가 본인이 맞다는것을 확인할것이다. 결국 매 사람은 그 카드를 반드시 소지할뿐아니라 그것을 사용하기 위한 비밀개인식별번호(PIN)도 알고 있어야 한다.

오늘 다목적신용카드 같은것을 가지고 있는 사람의 수는 비록 적지만 그 전자스마트카드는 빨리 다목적카드로 되여 상업자들과 은행을 비롯한 금융기관들에서 인정을 받음으로써 사람들이 가지고 다니는 카드(수자식인증서들과 비밀열쇠까지 포함하여)의 수를 줄일수 있게 될것이다. 금융기관들의 기반시설체계는 이미 다 되여 있으므로(ATM에 써붙인 공통적인 망기호들인 NYCE, Cirrus등을 볼것) 이번에는 몇가지의 표준안과 물리적인 카드가 하루밤사이에 나올수도 있다.

1999년 10월에 열린 제22차 전국년례정보체계보안대회에서 정보보안전문가들이 예측한바에 의하면 수자식인증서 그리고 지문과 같은 생체인식지표가 추가된 스마트카드는 3～5년내에 표준화될것이라고 한다. HIPAA정보안전 및 사적비밀조항의 준수마감날자가 2003년초까지이므로 안전한 원격정보통신을 보장하자면 보건산업이 제때에 그것을 도입해야 할 때가 왔다고 본다. 오늘의 보건계획과 병원신원증명서들은 래일의 스마트카드가 되여 환자들과 가입자들로 하여금 자기들의 기록정보를 제때에 갱신하며 시간약속을 하며 약처방을 떼는 일을 단번에 편리하게 할수 있게 할것이며 다른 그 누구도 자기처럼 위장하여 자기의 기록자료들에 비법적으로 접근하지 못한다는 확신을 가질수 있게 할것이다. 결국 이것이 바로 개인정보에 대한 보호인것이다.

결 론

정규적인 정보보안계획작성의 사회적 및 업무적필요성을 인식하는데서 보건산업은 력사적으로 국가경제의 그 어느 다른 부분보다도 뒤떨어 져 있다.

보건산업에서 인터네트를 급격히 사용하고 있는것으로 하여 부분적이지만 모든것이 점점 로출되여 가며 그리고 사적비밀보호에 대한 사회계의 관심과 우려가 날로 높아 가고 있는 이때에 정보보안을 요구하는 련방법인 HIPAA의 출현과 사적비밀보호문제로 하여 보건산업은 자기의 모습을 뚜렷이 보여 주고 있다. 이것은 정보보안계로 하여금 우리 모두와 관련되는 분야인 우리의 건강에 자기 지식과 기교를 남김없이 적용할 좋은 기회로 되고 있다.

제3장. 새로운 류형의 해커도구와 그에 대처한 방안

에드 슈코우디스

콤퓨터공격도구와 수법에서 첨단기술은 급속한 속도로 발전하고 있다. 봉사거부공격도구, 통과암호해독도구, 포구스캔도구, 엿보기도구(sniffer)와 루트키트(RootKit)와 같은 몇십년전부터 써오는 실효성 있고 전통적인 수많은 콤퓨터공격도구들에 아직도 골탕을 먹고 있다. 그러나 이 기초적인 도구들과 기법들중 많은것들이 지난 1～2년동안 개화기를 맞이하였는데 그것은 능력을 보다 강화하는 새로운 특징과 구조체계로 보강되였기때문일것이다. 해커들은 광범위하게 리용되는 규약들과 조작체계의 바로 심장부를 깊숙이 뚫고 있다. 해커들의 능력이 높아 가는것과 함께 그들의 콤퓨터공격도구들도 점점 사용하기 쉬워 지고 있다. 아하 이렇게 만들어 졌구나 하고 생각할 때에는 벌써 다른 새롭고 보다 쓰기 편리한 해킹도구가 출현하여 자기의 새로운 기능으로 강타를 먹일것이다. 인터네트에 약한 공격대상들이 많이 있는데다가 공격도구가 더 정교해 지고 쓰기 편리해 지는것으로 하여 오늘 우리는 해킹의 황금시대에 살고 있다.

이 장의 목적은 콤퓨터공격도구제작의 최근 동향을 개괄하자는것이다. 우리의 콤퓨터를 최대한 보호하기 위해서는 우리의 적들의 능력과 전술들을 잘 알아야 한다. 이 목적을 위하여 이 장에서는 분산공격, 적극적엿보기, 핵심부준위루트키트를 비롯한 공격도구의 일부 공격분야를 매 공격형태에 대처한 방안과 함께 보기로 한다.

분산형공격

콤퓨터공격도구의 창조에서 일차적으로 주목되는 추세의 하나는 분산형공격구조에로의 움직임이다. 원리적으로 공격자들은 인터네트자체의 분산된 능력을 재치 있게 리용하여 공격능력을 높이고 있다. 여기에서 책략은 명백하며 아마 이 분산형공격도구의 일부능력만 주어 지면 교묘하게 움직일것이다. 공격자는 보통 콤퓨터공격을 할 때 이 일을 많은 콤퓨터로 나누어 진행한다. 공격에 합세하는 콤퓨터체계가 더 많으면 많을수록 공격성공의 기회는 더욱 커진다. 이 분산형공격은 공격자에게 다음과 같은 유리한 점들이 있다.

- 탐지하기보다 어렵다.
- 공격자추적을 보다 어렵게 한다.
- 공격속도를 높임으로써 짧은 소요시간내에 소기의 목적을 달성한다.
- 한 공격자가 공격대상에서 더 많은 자원을 소비하게 한다.

그러면 공격자는 분산형공격개시에 필요한 이 모든 기계들을 어디에서 얻는가. 유감스럽게도 인터네트상에는 매우 약한 기계들이 굉장히 많으므로 언제든지 그것들을 쓸수 있다. 이러한 체계들을 소유하고 있는 사람들이나 관리하는 사람들은 대체로 판매업체로부터 보안프로그람들을 가져다 보강대책을 하기는 커녕 지함에서 그냥 꺼낼 때의 기정값설정을 그대로 쓰면서 설정을 안전하게 해놓지도 않고 있는 사람들이다. 각급 대학들과 각이한 규모의 회사들, 정부기관들과 가정들이 인터네트에 항상 접속되여 있으면서도 안전설정이 한심하여 공격자들의 좋은 먹이감으로 되기 쉽다. 수준이 낮은 공격자들도 전세계의 수백수천개의 콤퓨터를 쉽게 점령해 치울수 있다. 이 공격자들이 쓰는 도구는 Nessus회사의 취약성스캐너(http://www.nessus.org)와 같은 무료쏘프트웨어도구와 자체 스크립트로 만든 자동취약성스캐너이며 이것으로는 인터네트에서 두세번 큼직히 스캔해 낼수 있다. 공격자들은 취약한 콤퓨터체계들을 점령하기 위하여 밤낮으로 무차별적인 스캔을 진행한다. 적당한 수의 콤퓨터체계를 확보하면 이 불행한 콤퓨터들을 토대로 지정된 공격대상에 대한 분산형공격을 진행한다.

공격자들은 분산형체계에 맞게 여러 고전형콤퓨터공격도구들을 개량하였다. 이 장에서는 분산형봉사거부공격, 분산형통과암호해독, 분산형포구스캔 ,중계공격과 같은 가장 파급적인 분산형공격도구와 수법들을 보기로 한다.

분산형봉사거부공격

가장 인기 있고 가장 널리 리용되는 분산형공격기법의 하나는 분산형봉사거부(DDoS)공격이다. 이 공격시 공격자는 우선 수많은 콤퓨터체계들을 확보한 다음 매 콤퓨터에 좀비(Zombie)라고 하는 원격조종프로그람을 설치한다. 이 좀비는 매 콤퓨터들의 배경에서 조용히 기동하여 명령을 기다린다. 공격자는 어느한 콤퓨터에서 기동하는 어떤 전문화된 의뢰기프로그람을 사용하여 이 좀비체계들을 조종한다. 공격자는 하나의 의뢰기콤퓨터를 리용하여 방대한 수의 좀비들에 지령을 보내여 그것들이 동일한 행동을 동시에 수행하게 한다. 분산형봉사거부공격에서 가장 흔히 쓰이는 공동행동은 공격대상에 파케트를 동시에 다량적으로 보내는것이다. 모든 좀비들이 파케트를 동시에 다량으로 보내면 희생물이 된 그 콤퓨터는 갑자기 엉터리 없는 가짜전송흐름에 파묻히고 만다. 일단 그 콤퓨터의 통신선로용량이 고갈되여 버리면 그 어떤 합법적인 사용자의 신호도 그 콤퓨터에 도달하지 못하게 되여 결국 봉사거부가 생긴다.

분산형봉사거부공격의 방법이 세상에 요란히 선보인것은 2000년 2월 몇개의 유명한 인터네트싸이트들이 이러한 공격을 받았을 때였다. DDoS도구들은 끊임없이 발전하여 그 특성이 이제는 점점 더 참기 어려운것으로 되고 있다. 최신형태의 DDoS공격은 넓은 범위의 위장능력까지 가지고 공격자의 콤퓨터와 좀비들사이 그리고 좀비들과 공격대상콤퓨터사이의 모든 통신을 다 가짜원천주소로 진행한다. 그러므로 파케트범람이 시작되면 수사관들은 사건추적을 매 경로기의 구간을 하나씩 차례로 훑어 피해자콤퓨터부터 매 좀비들을 조사해야 한다. 좀비들을 다 훑어 걷어 내면 그다음에는 여러가지 반사경로들이 다중적인 인터네트봉사제공자들을 전반적으로 훑어 가며 좀비들로부터 범인콤퓨터까지 추적해 나가지 않으면 안된다. 또한 DDoS공격도구들은 암호화기법으로 좀비들의 위치를

위장해 치우고 있다. 기성세대의 DDoS도구들을 보면 대부분의 범인콤퓨터쏘프트웨어에는 좀비들의 망주소명단이 있는 파일이 있었다. 이 의뢰기콤퓨터를 발견하면 수사팀은 재빨리 좀비들의 위치를 알아 내여 제거하게 되여 있었다. 최근 이 좀비주소목록파일을 암호화해 놓기때문에 새 세대 DDoS도구를 가지고는 범인콤퓨터를 추적하였다 하더라도 좀비들의 위치를 알아 낼수 없게 되여 있다.

분산형봉사거부공격에 대처할 방안들

DDoS공격까지 포함한 파케트범람에 대처하기 위하여서는 주요련결망들이 충분한 대역과 예비공간을 확보하여 단순한 공격들을 물리칠수 있게 하는것이 중요하다. 공격자에 의하여 모든 하위련결망이 쉽게 차단되기때문에 만약 어느 한 련결망이 해당 기관에서 사활적인 경우에는 예비T1련결이라도 가지고 있는것이 좋다.

이 기초대역을 가지면 최저급의 공격자들은 제거할수 있지만 100～1,000대의 콤퓨터에 좀비들을 설치하고 목표물로 지향시키는 공격자들을 막아 낼 충분한 대역을 확보할수는 없다는것을 알아야 한다. 만일 인터네트에 련결된 그 콤퓨터를 쓰는 문제가 기업전반에 사활적인 경우에는 보충적인 기술을 도입하여 DDoS공격을 처리할수밖에 없다. 기술적견지에서는 전송흐름구성도구를 고려하는 수가 있을수 있다. 이 도구를 쓰면 들어 오는 대화회수를 조절하여 자기 봉사기의 부담을 덜어 줄수 있다. 물론 굉장한 량의 좀비군이 한개 선로로 무리 지어 범람해 오면 전송흐름구성도구도 마비되여 버릴수 있다. 그러므로 공격이 현재 진행중인가를 알기 위하여 침입검출체계(IDS)를 리용해야 한다. 이 IDS는 일종의 망도적경보장치로서 IDS자료기지에 기억된 일반공격표적들과 대조하여 보는 방법으로 망전송흐름을 감시한다. 공정적인 견지에서는 IDS에서 나오는 이러한 경보신호를 처리할수 있는 사건대응팀을 가동시켜 대기시켜야 한다. 업무에 필수적인 인터네트련결선로를 위해서는 인터네트봉사제공자(ISP)의 사건대응팀을 찾기 위한 무선전화 및 호출기번호들을 가지고 있어야 한다. DDoS공격이 시작되면 자기 기관의 사건대응팀은 신속정확히 인터네트봉사제공자의 사건대응팀의 무력을 안내하고 인도해 줄수 있어야 한다. 발동이 걸리면 인터네트봉사제공자는 자기의 망에 려과장치들을 전개하여 적극적으로 밀려 오는 DDoS공격을 막을수 있게 된다.

분산형통과암호해독

통과암호해독수법은 최근 몇해동안 성행해 온 또 하나의 해킹기법으로서 분산형공격에서는 그 기능이 계속 강화되고 있다. 이 수법은 현대적인 콤퓨터체계들(UNIX와 Windows NT와 같은)에는 인증으로 쓰는 암호화된 통과암호들을 담은 자료기지가 있다는 사실에 기초하여 착안한 기법이다. Windows NT에는 통과암호들이 SAM자료기지에 기억되여 있다. UNIX체계에는 통과암호들이 /etc/passwd나 /etc/shadow파일들에 있다. 사용자가 체계에 가입하면 콤퓨터는 사용자에게 통과암호를 물어 보고 사용자가 입력한 값들을 암호화하여 이미 암호화되여 보관된 통과암호와 비교한다. 일치하면 사용자의 망가입은 허용된다.

통과암호해독의 원리는 간단하다. 암호화된 통과암호파일을 훔치고 통과암호를 추측하고 그 추측한것을 암호화한 다음 훔쳤던 암호화된 통과암호파일에 들어 가 있는 값과 비교해 본다. 만일 추측값을 암호화한것이 암호화된 통과암호와 일치하면 공격자는 통과암호를 알아 낸것이나 같다. 만일 두 값이 일치하지 않으면 공격자는 추측을 달리 한다. 사용자통과암호는 사용자의 신원내용과 사전에 있는 단어, 기타 문자들로 추측하여 흔히 조합할수 있으므로 이 기법이 통과암호를 밝혀 내는데서 대체로 매우 성공적이다.

전통적인 통과암호해독도구들은 추측, 암호, 비교, 순환고리를 자동화하여 통과암호를 신속정확히 결정할수 있게 한다. 이 도구들은 사용자신원, 사전용어들, 강제력을 리용하여 가능한 모든 조합을 구성하고 추정하는 방법으로 통과암호를 밝혀 낸다. 보다 성능높은 통과암호해독도구들은 사전에 있는 표준단어들의 앞뒤에 강제식방법으로 문자들을 붙였다뗐다 하면서 복합공격을 가하기도 한다. 대부분의 통과암호들은 단순히 어떤 사전단어의 앞이나 뒤에 특수문자들을 몇개 덧붙여 놓은것이기때문에 복합공격을 들이대면 성공률이 상당히 높아 진다. 일부 성능이 가장 높은 전통적인 통과암호해독도구들로는 Windows NT용 L0phtCrack(http://www.l0pht.com에서 구입가능함)와 UNIX와 Windows NT를 비롯한 여러가지 체계들에서 쓰는 John the Ripper(http://www.openwall.com에서 구입가능함)가 있다.

통과암호해독에서는 속도가 기본문제이다. 통과암호추측값을 더 짧은 시간내에 더 많이 창조하고 검사할수록 공격자는 그만큼 더 많은 통과암호를 알아 내게 된다. 전통적인 통과암호해독도구들은 이 속도문제를 해결하기 위하여 추측값을 암호화하는데 쓰이는 암호알고리듬실행을 최량화하고 있다. 공격자들은 보다 높은 속도를 위하여 암호해독과정의 작업량을 수많은 콤퓨터들에 분산시키는 방법을 적용할수 있다. 공격자들은 신속정확히 통과암호를 해독하기 위하여 인터네트에 널려 있는 수백수천대의 콤퓨터들을 장악하고 동원하여 하나의 통과암호파일을 뚫고 들어 가 휘저어 놓기도 한다.

분산형통과암호해독을 실행하기 위하여 공격자는 전통적도구를 리용하여 작업량을 수동적으로 하나하나 나눈다. 실례로 어느 한 공격자가 10개의 통과암호를 가진 암호파일을 해독한다고 하자. 공격자는 한 부분에 하나의 통과암호가 들어 가게끔 이 파일을 10개의 부분으로 갈라서 10대의 콤퓨터에 나누어 준다. 매 콤퓨터에서는 전통적암호해독도구가 동작하여 자기가 맡은 하나의 통과암호를 해독한다. 혹은 10개의 모든 통과암호를 매 콤퓨터에 분배하고 매 기계의 해독도구가 같은 사전의 서로 다른 부분이나 일정한 문자만 강제식으로 제각기 분석해 내도록 할수도 있다.

수동으로 작업량을 쪼개는 전통적인 통과암호해독도구를 사용하는것이외에도 최근 몇년간에 자체로 만든 몇가지 분산형통과암호해독도구도 나왔다. 이 도구들은 자동적으로 여러 콤퓨터들에 작업량을 분배하며 공격이 진척됨에 따라 콤퓨터지원을 조정하기도 한다. 가장 대중화된 일련의 분산형통과암호해독도구로서는 Mio–Sta와 Saltine Cracker를 들수 있는데 이것들은 다 http://packetstorm.security.com/distributed에서 구입할수 있다.

분산형통과암호해독에 대처한 방안들 분산형통과암호해독에 대처한 방어대책들은 실지 전통적인 통과암호해독에 대처한 방안과 같다. 즉 체계에 있는 약한 통과암호들은 제거해 버리는것이다. 분산형해독에서는 암호해독속도가 높기때문에 비분산형암호해독이 지배적이던 이전보다 통과암호를 더 추측하기 힘들게 하여야 할 필요가 있다. 매 통과암

호의 길이를 최소길이보다 더 길게(아홉자리문자렬보다 더 길게) 하며 매 통과암호에 수자, 문자, 특수기호들을 포함시키는것을 초보적인 원칙으로 삼도록 하는것이 좋을수 있다. 모든 사용자들이 이 원칙을 알게 하며 예측불가능한 통과암호의 중요성을 강조해 주는것이 비결이다. 또한 이러한 통과암호방책을 실시하기 위해서는 인증봉사콤퓨터에 통과암호려파도구들을 설치할수도 있다. 어느 한 사용자가 새로운 통과암호를 개설하면 이 도구들이 그 통과암호가 통과암호방책에 부합되는가를 검열하게 해야 한다. 통과암호가 너무 짧거나 수자, 문자, 특수문자들을 포함하지 않는 경우 사용자에게 다른 통과암호를 만들것을 요구할수 있다. Windows NT의 Resource Kit에 있는 passfilt.dll파일과 UNIX체계의 passwd+프로그람은 일련의 제3자적인 보충적인증프로그람제품들이 그러하듯이 이런 특성을 제공하고 있다. 또한 매우 예민한 기밀보장환경에서는 아예 표준적인 통과암호제도를 없애 버리고 통표(token)에 의한 접근기술을 도입하는것도 나쁘지 않다.

마지막대책으로서는 보안담당자들이 정기적으로 통과암호해독도구를 리용하여 자기기관의 사용자들의 통과암호를 검열해봄으로써 공격자가 손을 쓰기전에 취약한 고리들을 찾아 내는것이다. 취약한 통과암호들이 발견되면 그 사용자들에게 보다 강한 통과암호를 쓸것을 통지해 주는 명백하고도 허용된 공정이 있어야 할것이다. 기관내적인 암호해독사업을 하기전에 경영진이 이 중요한 보안계획을 리해하고 지지하도록 해야 하며 해당 승인을 반드시 사전에 받아 두는것을 잊지 말아야 한다. 경영진의 동의를 받지 못하고 이 사업을 시작하면 자기의 직업에 부정적영향을 미칠수 있다.

분산형포구스캔

분산형방법에 적합한 또 하나의 공격수법은 포구스캔이다. 포구는 전송조종규약(TCP)과 사용자데타그람규약(UDP)에서 중요한 하나의 개념이며 이 두 규약들은 거의 모든 망봉사에서 사용되고 있다. 망에서 TCP와 UDP자료흐름을 받는 매 봉사기는 하나 혹은 그이상의 포구접속을 기다린다. 이 포구들은 콤퓨터에 있는 자그마한 가상출입문과 같아서 여기로 자료파케트들이 들어 가고 나가고 한다. 포구번호들은 파케트들이 향하고 있는 한 체계의 주소역할을 한다. 체계의 행정관리자가 망봉사가 어느 포구를 기다리겠는가를 설정은 할수 있지만 대부분의 봉사들은 보통 잘 알려 진 포구를 기다림으로써 의뢰기프로그람으로 하여금 어디로 그 파케트들을 보내겠는가를 알게 한다. Web봉사기들은 대체로 TCP포구주소 80을 기다린다면 인터네트우편봉사기들은 TCP포구주소 25를 기다린다. 령역이름봉사기는 UDP포구주소 53의 질문을 기다린다. 수백개의 각종 포구들은 http://www.ietf.org/rfc.html에서 구입할수 있는 문건인 RFC 1700에서 볼수 있는바와 같이 각이한 봉사형태에 배당되여 있다.

포구스캔은 목표체계에 있는 각이한 포구들에 파케트들을 보내여 어느 포구가 봉사신호를 기다리고 있는가를 결정하는 과정이다. 이것은 목표체계의 문들을 하나하나 두드려 보고 어느것이 열려 있는가를 알아 내는것과 류사하다. 목표체계에서 어느 포구가 열려 있는가를 아는 방법으로 공격자는 그 기계에서 실행되고 있는 봉사형태를 알수 있게 된다. 그다음 공격자는 이 열려 진 포구들과 관련되는 봉사에 공격을 집중할수 있게 된다. 또한 목표체계에서 열려 진 매 포구는 공격자에게 있어서 가능한 침입점으로도 된다.

공격자는 그 콤퓨터에 대하여 스캔하고 TCP포구 25와 UDP포구 53이 열려 있음을 확인한다. 그 결과를 보고 침입자는 그 콤퓨터가 우편봉사기이며 DNS봉사기일수 있다는것을 안다. 현재 방대한 수의 전통적인 포구스캔도구들이 나와 있지만 가장 강력한 도구는 Nmap도구로서 http://www.insecure.org에서 구입할수 있다.

포구스캔이 보다 심도 있는 공격의 전조로 되기때문에 보안관계자들은 IDS도구들을 써서 포구스캔을 조기경보신호로 하여 이것을 검출해 낼수 있다. 대부분의 IDS는 포구스캔을 인식하는 고유한 기능을 가지고 있다. 한 파케트가 주어 진 원천으로부터 어느 한 포구를 거쳐 도착하고 그후에 다른 파케트가 같은 원천으로부터 다른 포구에 도착하고 또 다른 파케트가 또 다른 포구에 도착하면 IDS는 신속히 이 파케트들을 호상 확인하는 방법으로 포구스캔을 검출할수 있다. 이런 통신방식은 그림 3－1에서 왼쪽에 있는것과 같으며 여기에 포구번호가 원천망주소공격을 위해 배치되여 있다. IDS는 이 스캔을 쉽게 포착한 다음 경보신호(혹은 행정책임자에게는 전자우편)를 보낼수 있게 된다.

그러면 공격자가 분산형포구스캔을 할 때 어떤 현상이 일어 나는가를 보자. 하나의 주소로부터 다량의 파케트를 단번에 련발사격을 할 대신에 공격자는 이 스캐닝에 많은 콤퓨터들이 참가하게 설정해 놓을것이다. 여러 콤퓨터들은 협동하여 스캔하면서 목표콤퓨터에 있는 흥미 있는 포구들을 모두 검사하여 결과를 보내면 공격자는 이것들을 서로 련관시킨다. 전통적인 포구스캔의 형태를 감시하는 IDS는 이 공격을 탐지하지 못한다. 그래서 그림 3－1의 오른쪽에서 보는바와 같이 들어 오는 파케트들의 형태는 산발적인것으로 보이게 된다. 이런 방법으로는 분산형포구스캔을 검출하기 더욱 어렵다.

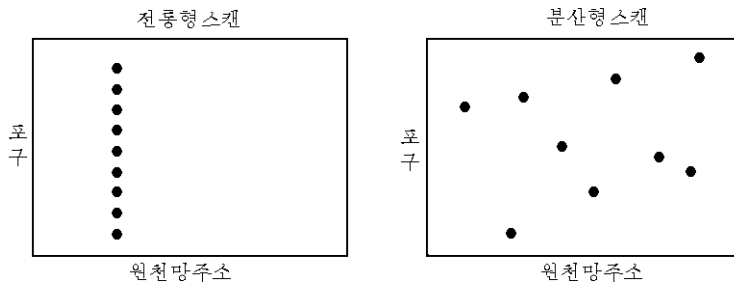



그림 3－1. 전통형스캔과 분산형스캔

물론 IDS체계는 원천주소가 아니라 목표주소(즉 파케트들이 가는 곳의 주소)에 초점을 집중하면 분산형포구스캔을 탐지해 낼수 있다. 가령 수많은 콤퓨터들에서 갑자기 어느 한 콤퓨터에 있는 여러 포구들에 파케트들을 보내면 IDS는 포구스캔이 진행중인것으로 추측할수 있다. 그러나 공격자는 분산형스캔을 장기적으로 진행하는 식으로 탐지가능성을 더욱 약화시킨다. 분산형스캔을 보다 오랜기간(례하면 한주 혹은 한달간) 진행하면 공격자가 I-DS를 교묘히 속여 넘길수 있는 가능성이 상당히 커진다. 분산형포구스캔할 때 공격자추적이 더욱 불가능한것은 또한 스캔작업을 수행하는 콤퓨터가 공격자의 소유가 아닌 여러 곳에 있기때문이다.

여러가지 분산형포구스캔도구들이 현재 나돌고 있다. 어떤 침입자는 그 이름을 보아

도 명백한 phpdistributedportscanner프로그람을 쓸수 있는데 이 도구는 자그마한 스크립트로서 Web봉사에 태워 스캔을 진행할수 있다. 공격자가 물리평면가능(PHP–enabled)Web봉사기를 점령할 때마다 그 봉사기에 스크립트를 떨구어 그것을 리용하여 다른 콤퓨터들에 대한 스캔을 진행한다. 공격자는 HTTP요구명령을 리용하여 각이한 Web봉사기들에서 실행되는 개별적인 스캐닝스크립트들과 호상 련계를 가진다. 모든것이 Web상에서 진행되므로 분산형포구스캔은 실행시키기 상당히 쉽다. 이 스캐닝도구를 구입할수 있는 곳은 http://www.digitaloffense.net:8000/phpDistributedPortScanner/이다. 다른 형의 분산형포구스캐너들은 의뢰기/봉사기 구조에 기초한것으로서 대표적인것들로는 Dscan(http://packetstorm.security.com/distributed에서 구입가능함)과 SIDEN(http://siden.sourceforge.net에서 구입가능함)을 들수 있다.

분산형포구스캔에 대처한 방안들 최선의 방도는 자기콤퓨터체계에 있는 필요 없는 봉사체계들을 몽땅 닫아 버리는것이다. 자기 체계의 유일한 목적이 HTTP와 HTTPS를 통한 통신을 하는 Web봉사기운영이라면 TCP포구 80과 TCP포구 443만 열어 놓고 있으면 되는것이다. Web봉사기로 리용되는 기계이므로 거기서 가동하는 우편봉사체계가 필요 없다면 우편봉사기기능은 비활성으로 선택하는 식으로 체계설정을 해놓을수 있다. 만일 X Windows체계가 필요 없다면 그 프로그람을 정지시키면 된다. 기타 쓰지 않는 모든 봉사체계들을 정지시켜 해당한 포구들을 닫아야 한다. 안전한 체계설정문건을 작성하여 기관의 모든 체계담당자들이 단계별로 쓸수 있는 봉사기안전구축조치를 취해야 할것이다.

보충적으로 말하여 IDS의 기능을 항상 갱신하도록 하는것이 중요하다. 대부분의 IDS 판매업체들은 대체로 한달에 한번씩은 갱신된 새로운 형태의 공격표적들을 배포한다. 이 공격표적의 구입이 가능하면 신속히 성능검사하고 IDS에 추가설치하여 최신공격수법을 검출할수 있도록 해야 한다.

중계공격

분산형공격수법의 마지막형태는 인터네트상에서 콤퓨터별로 정보를 계속 중계시킴으로써 공격자의 실지원천콤퓨터를 추적할수 없게 보호하도록 하는 수법이다. 흔히 예상할수 있듯이 대부분의 공격자들은 잡히기를 원하지 않는다. 공격자는 자기와 타격대상사이에 련계를 모호하게 하는 기만적인 우회층을 많이 쌓아 놓음으로써 추적되지 않으려고 한다. 공격자가 인터네트에 접속되여 있는 여섯대의 콤퓨터를 장악하여 타격대상에 대한 공격을 하려 한다고 보자. 공격자는 여섯대의 콤퓨터에 파케트방향바꾸기프로그람을 각각 설치한다. 첫 콤퓨터가 해당 포구로 받은 임의의 파케트를 두번째 콤퓨터에 보낸다. 두번째 콤퓨터는 그것을 세번째에 보내는 식으로 계속되여 마지막에는 목표에 이른다. 매 체계는 공격자의 송신에 복무하는 하나의 중계망에 있는 고리로 된다. 만일의 경우 공격을 탐지하면 수사팀은 매 중계점들을 거꾸로 밟아 추적하여 공격자를 찾아 낼것이다.

공격자들은 대체로 세계적으로 널려 있는 수많은 콤퓨터들을 장악하여 중계망을 구성한다. 또한 수사관들의 추적을 피하기 위해 중계망의 매점들이 지리적으로나 정치적으로나 차이가 크고 쓰는 언어가 완전히 다른 지역에 놓이도록 한다. 실례로 첫 중계는 미국에서, 둘째 중계는 중국에서, 셋째 중계는 인디아에서, 넷째 중계는 파키스탄에서 그리

고 마지막공격은 이라크에서 하여 결국 미국에 있는 대상들을 공격하게 할수 있다. 매 중계점들에서 수사관들은 서로 다른 언어로 말하는 사람들, 나라마다 친절치 못한 태도, 사법관계의 큰 차이로 하여 큰 싸움을 치르지 않으면 안되게 된다.

중계공격실행에 흔히 쓰이는 매우 유연한 도구는 Netcat로서 UNIX용은 현재 http://www.l0pht.com/users/l0pht/nc110.tgz에서 구입할수 있으며 Windows NT용은 http://www.l0pht.com/~weld/netcat/에서 구입할수 있다. 다른 하나의 인기 있는 중계도구는 Redir로서 http://oh.verio.com/～sammy/hacks에서 구입할수 있다.

중계공격에 대처한 방안들 중계공격의 대부분은 기관내망밖에서 진행되는것이므로 이 공격에 대처할 방도는 거의 없다. 공격이 미치기전에 파케트들을 서로 주고받고 하는 콤퓨터들의 행동을 미리 막을수는 없는것이다. 최선의 방도는 모든 안전조치들을 보강하고 필요 없는 봉사는 다 닫아 버려 체계의 안전성을 기하는것이다. 보충적으로 사법관계일군들과 협력하여 이러한 공격을 조사하는것도 중요하다.

적극적엿보기

엿보기는 력사가 더 오랜 또 하나의 수법으로서 현재 새로운 능력으로 빨리 확장되고 있다. 전통적인 엿보기도구들은 망상에서 전송정보를 수집하는 단순한 프로그람이다. 사용자가 엿보기프로그람을 어느 한 콤퓨터에 설치하면 그 콤퓨터는 자기에게 오는것이든 다른 곳에 가는것이든 관계없이 자기 콤퓨터의 망대면부를 지나가는것이라면 모든 자료를 다 잡는다. 망관리자가 이 도구를 쓰는 경우 전송통로를 헛갈린 파케트들을 잡아 망의 고장을 퇴치할수 있다. 공격자가 쓰는 경우 망에서 전송되는 통과암호, 파일들, 전자우편 등과 같은 기밀성이 있는 자료들을 손에 넣을수 있게 된다.

전통형엿보기

전통형엿보기도구들은 피동적인것이여서 자기 망에서 전송자료가 지나가기를 참을성있게 기다리다가 어떤 자료가 도착하면 잡는 방식이다. 이 피동적수법은 일부 망형태들에서는 효과가 좋다. 방대한 수의 국부망(LAN)형성에 리용되는 보편적인 기술인 전통형이써네트는 동시전송수단이다. 이써네트집선기들은 전통형이써네트 LAN을 구축하는데 쓰이는 장치이다. 이 LAN상의 어느 한 콤퓨터에 보내는 모든 자료는 LAN에 련결되여 있는 모든 콤퓨터들에 동시전송된다. 따라서 전통형엿보기도구만 있으면 동일한 LAN상에서 서로 다른 콤퓨터들사이에 오가는 그 어떤 자료든지 훔쳐 볼수 있다. 전통형엿보기공격을 하기 위해서는 공격자가 그 LAN상의 어느 한 콤퓨터를 장악하고 거기에 도청프로그람을 설치하면 그 망에 소속된 모든 콤퓨터들에 가는 전송자료들을 다 손에 넣을수 있다. 가장 좋은 전통형엿보기도구들로서는 Snort(http://www. snort.org에서 구입가능함)와 Sniffit(http://reptile.rug.ac.be/～coder/sniffit.html에서 구입가능함)가 있다.

전통형엿보기에 대처한 가장 보편적인 방어대책으로는 교환기를 LAN에 설치하는것

이다. 동시방송수단인 이써네트집선기와는 달리 이써네트교환기는 목적한 대상에만 자료를 보낸다. 이 이써네트교환기가 해당 대상콤퓨터에만 자료를 보내기때문에 그 망의 다른 콤퓨터에서는 그 자료를 볼수 없다. 다른 하나의 방어기법으로서는 자료를 암호화하는것이다. 공격자에게 암호해독열쇠가 없으면 아무리 망에서 자료를 엿보거나 훔쳤다 해도 그 내용을 알수 없게 된다. 가장 많이 쓰이는 두가지 암호규약들로는 Web자료통신용안전소케트층(SSL)과 명령렬쉘방식의 체계접근보호용안전쉘(SSH)이다.

적극적엿보기에 대처한 방도

방어대책들은 설치하기 쉽고 효과가 있으나 그에 대항하여 공격자들은 여러가지 수법들을 개발해 내였다. 적극적엿보기라고 통칭되는 이 기법들은 망에 전송자료들을 주입하여 다른 방법으로는 훔치기 힘든 자료들을 공격자들이 얻을수 있는 방법이다. 그중 가장 능력이 높고 활동적인 프로그람이 Dsniff인데 현재 http://www.monkey.org/～dugsong/dsniff/에서 구입이 가능하다. 망에 전송자료를 주입함으로써 엿보기를 하는 Dsniff의 방식들에는 MAC주소범람, 허위ARP자료전송, 위조DNS응답 그리고 SSL에 대한 중개인공격 등이 있다.

매체접근조종(MAC)주소범람 이 이써네트교환기는 매체접근조종주소에 기초하여 LAN에서 어디로 자료전송을 할것인가를 결정한다. MAC주소는 고유한 48bit수자로서 매 이써네트카드에 배당되여 있다. MAC주소란 LAN을 구성하는 매 콤퓨터의 망접속하드웨어주소를 말한다. 이써네트교환기는 어느 단자들이 어느 MAC주소와 련결되여 있는가를 알기 위하여 교환기의 LAN의 자료흐름상태를 항상 감시한다. 실례로 교환기는 MAC주소 AA:BB:CC:DD:EE:FF로부터 오는 전송자료가 1번단자에 온다는것을 알수 있다. 교환기는 이 정보를 기억하고 이 MAC주소로 오는 모든 자료들을 오직 이 첫 단자에만 련결시켜준다. 이런 식으로 LAN의 다른 콤퓨터들의 망대면부와 관련한 MAC주소들을 자동적으로 탐지하고 해당 자료들을 해당 콤퓨터에만 보낸다.

가장 간단한 적극적엿보기기법의 하나는 LAN에 가짜MAC주소를 가진 자료들을 다량 주입하는것이다. 공격자는 LAN이 어느 한 콤퓨터에 설치된 어떤 프로그람을 리용하여 임의로 만들어 낸 MAC주소들을 가진 파케트들을 생성하여 교환기에 주입한다. 교환기는 들어 오는 모든 자료들의 MAC주소들을 다 기억하려고 한다. 결국 교환기의 기억이 그 가짜주소들을 기억하는데 다 소모되여 버릴것이다. 기억이 다 차면 일부 교환기들은 할수 없이 전송자료들을 LAN의 모든 콤퓨터들에 다 보내는 방식으로 들어 가게 된다. 그렇기때문에 공격자들은 MAC주소를 다량 주입하여 교환기를 《폭격》함으로써 교환기가 모든 전송자료들을 LAN의 모든 콤퓨터들에 보내지 않으면 안되게 만든다. 그다음에는 전통적인 엿보기도구들을 리용하여 LAN에서 자료를 손에 넣을수 있게 한다.

위조ARP자료전송 우에서 본것처럼 일부 교환기들은 MAC범람에 의하여 모든 콤퓨터들에 자료전송을 다 해줄수도 있지만 그렇게 하지 않는 교환기들도 있다. MAC주소가 범람할 때 이러한 교환기들은 LAN에서 이미 알아 두었던 초기 MAC주소들을 기억하여 주소가 범람되는 전 기간 이 주소들을 리용한다. 공격자가 MAC주소를 범람시켜도 교환기는 끄떡 없다. 그러나 공격자는 주소변환규약(ARP)에 기초한 다른 새로운 형의 자료흐름

을 주입함으로써 LAN에 재공격을 시도할수 있다.

ARP는 인터네트규약(IP)주소로 LAN상의 MAC주소를 찾기 위한 주소목록작성에 리용된다. LAN상에서 한 기계가 다른 기계에로 자료를 전송할 필요가 있다고 하면 그 기계는 수신할 기계의 IP주소로 파케트를 만든다. 그러나 그 IP주소는 다만 그 대상기계에 대한 체계설정에 지나지 않는다. 그러면 파케트를 보내야 할 기계는 LAN상의 어느 하드웨어에 그 파케트를 보내야 하는가. ARP가 바로 대답이다. LAN상에 있는 한 콤퓨터가 IP주소 10.1.2.3에 보낼 파케트를 가지고 있다고 하자. 그 콤퓨터는 LAN상에 ARP요구신호를 보내여 어느 망대면부가 IP주소 10.1.2.3과 련결되여 있는가를 물어 본다. 이 IP주소를 가진 기계는 ARP응답신호로 《IP주소 10.1.2.3은 MAC주소 AA:BB:CC:DD:EE:FF와 련결되여 있음》이라는 요지의 내용을 내보낸다. 이 신호를 받은 기계는 앞으로의 참고를 위해 이 IP주소와 MAC주소의 련관내용을 ARP대응표라고 부르는 표를 자기 기계안에 보관해 놓는다. 그다음 이 MAC주소를 가진 망대면부에 이 파케트들을 보낸다. 이렇게 ARP는 IP주소를 MAC주소로 변환하여 LAN상에서 해당 자료들을 해당 기계에 보내주는데 쓰인다. 결과값들은 LAN상에서 다시 ARP를 전송하지 않도록 자기 콤퓨터에 ARP대응표로 보관해 놓는다.

ARP는 《무료ARP》라고 하는 기능도 지원한다. 이 무료ARP로는 어느 기계가 ARP요구신호를 보내오지 않아도 ARP응답신호를 보낼수 있게 된다. 많은 콤퓨터들은 LAN상에서 성능을 향상시키는데 도움이 되는 이 ARP자료들을 자기의 ARP표에 포함시키려고 한다.

다른 하나의 적극적엿보기형태에서는 공격자가 그림 3−2에서 보는것과 같이 허위적인 무료ARP통보문을 리용하여 자료전송방향을 바꾸어 교환기가 달린 LAN상에서 엿보기를 진행한다. 그림에서 LAN상에 있는 공격자의 콤퓨터는 검은 모자를 씌워 놓은것이다.

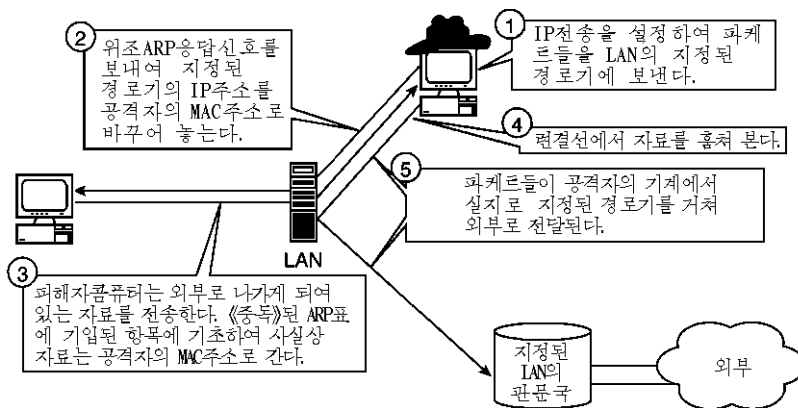



그림 3−2. 무료ARP통보문을 사용하여 교환기
환경에서 적극적엿보기를 실행하기

그림 3−2에서 보는 공격단계는 다음과 같다.

1. 공격자는 공격자콤퓨터에서 IP전달을 한다. 교환기에서 공격자의 콤퓨터에로 향해 진 파케트들이 LAN경로기에 다시 향해 진다.
2. 공격자는 무료ARP통보문을 공격대상으로 지적한 콤퓨터에 보낸다. 바로 이 콤퓨터에서 외부로 나가는 통신내용을 공격자가 노리는것이다. 보내여 진 ARP통보문은 LAN경로기의 IP주소를 공격자자신의 MAC주소로 변환시켜 준다. 대상콤퓨터는 이 허위적인 ARP신호를 받아서 자기 ARP표에 기록한다. 대상콤퓨터의 ARP표는 이젠 허위자료에 의해 《독약》을 먹은셈이다.
3. 대상콤퓨터는 외부로 내보내게 된 전송자료를 보낸다. 콤퓨터는 자기의 ARP표를 참조하여 LAN경로기의 주소를 알아 보려고 한다. 표에서 찾은 MAC주소는 공격자의 주소로 되여 있다. 밖으로 내보내는 모든 자료는 공격자의 콤퓨터로 간다.
4. 공격자는 회선으로부터 전송자료를 훔쳐 본다.
5. 첫 단계에서의 IP전송을 다시 하여 공격자의 콤퓨터에서 나오는 모든 자료전송을 LAN의 기정경로기에 가게 방향을 바꾸어 준다. 이 경로기는 자료를 외부에 보낸다. 이렇게 되여 피해자콤퓨터는 자료를 외부에 보낼수 있게 되나 외부로 가는 도중에 이렇게 공격자의 콤퓨터에 의해 중도에서 훔쳐 지게 된다.

이런 과정을 거쳐 공격자콤퓨터는 해당 콤퓨터에서 외부로 전송되는 자료를 몽땅 엿볼수 있게 된다. 그런데 공격자가 교환기에는 그 어떤 교정조작을 전혀 하지 않는다는 사실에 주목할 필요가 있다. 공격자는 대상콤퓨터의 ARP표만 조작하여 LAN교환기망에서 자료를 엿보는것이다. ARP자료전송과 해당 MAC주소정보전송이 LAN을 통해서만 진행되기때문에 해당 LAN에 있는 콤퓨터를 공격대상으로 삼는 경우에만 이 엿보기수법이 가능할수 있다.

위조DNS응답신호 파케트들을 망에 주입하여 LAN바깥까지의 전송자료들을 훔쳐 보는 이 수법에는 령역이름체계(DNS)를 조작하는것을 기본방법으로 삼고 있다. ARP가 LAN상에서 IP주소를 LAN상의 MAC주소로 련결시키는데 쓰는것이라면 DNS는 일반망상에서 령역이름을 IP주소로 련결시켜 주는데 쓰이는것이다. 사용자가 의뢰자쏘프트웨어 례하면 Web열람기에 www.skoudisstuff.com이라고 입력하면 사용자의 체계는 DNS봉사기에 문의신호를 보낸다. 이 DNS봉사기는 망의 저쪽에 있는 다른 LAN에 위치하여 있다. 이 문의신호를 받자마자 DNS봉사기는 자기 구성파일에 있는 해당 정보를 찾아서는 IP주소(례하면 10. 22. 12. 41)를 가진 사용자콤퓨터에 DNS응답신호를 보낸다. DNS봉사기가 사용자를 위해 령역이름을 IP주소로 바꾸어 준다.

공격자들은 가짜DNS응답신호를 목표로 된 콤퓨터에 보냄으로써 자료통신의 방향을 바꾸어 놓는다. 무료DNS응답신호 같은것은 없지만 이 수법에서 목표콤퓨터와 DNS봉사기사이에 있는 망우의 그 어떤 지점에 앉아 있는 공격자는 회선에서 DNS문의신호를 엿볼수 있게 된다. 목표콤퓨터에서 오는 DNS문의신호를 보자마자 공격자는 그 목표콤퓨터에 자기콤퓨터의 IP주소를 담은 가짜DNS응답신호를 보낸다. 속히운 목표콤퓨터는 자기가 지금 해당 봉사기와 통신을 주고 받는것으로 생각하고 자기파케트들을 이 IP주소로 보내게 된다. 결국 정보는 공격자의 콤퓨터로 도착한다. 공격자는 전통적엿보기도구로 자료를 본 다음 목적지인 해당 봉사기에 그 자료를 중계해 준다.

SSL에 대한 중개인공격 가짜DNS응답을 망에 주입하는것은 특히 안전한 Web접근에 쓰이는 SSL(안전소케트층)과 같은 암호화규약에 대한 중개인공격시에 강력한 수법으로 된다. 본질상 공격자가 가짜DNS응답신호를 목표에 보내여 새로운 SSL과정이 공격자의 기계를 통하여 설립되도록 하는 수법이다. 그림 3－3에서 보는바와 같이 공격자는 전문적인 중계도구를 리용하여 두가지 암호화과정을 거친다. 즉 의뢰기(목표물)와 공격자사이 그리고 공격자와 봉사기사이의 두 대화조종과정이다. 두 과정사이에 자료가 오가는 과정에 공격자는 그것을 명백한 본문형태로 보게 된다.

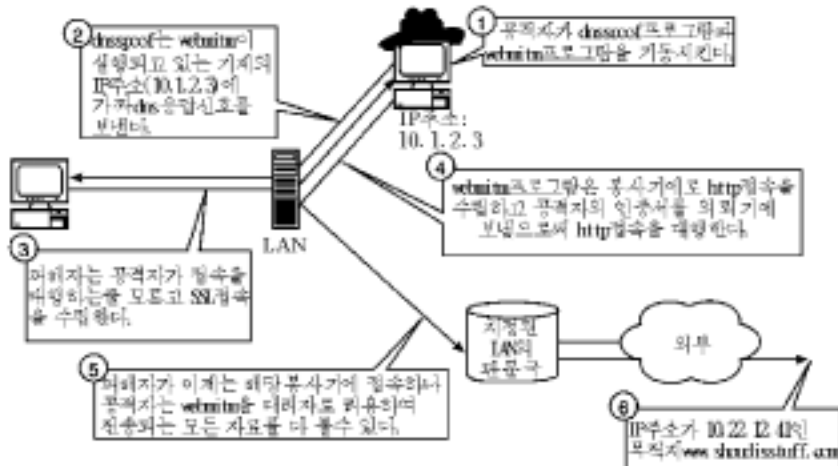



그림 3－3. DNS응답신호를 주입하여 SSL전송내용을
방향 바꾸어 훔치는 수법

그림 3－3에서 제시된 대화조종과정들은 다음과 같다.

1. 공격자는 가짜DNS응답신호를 보내는 Dsniff의 dnsspoof프로그람을 기동시킨다. 보충적으로 공격자는 Web Monkey–in–the Middle의 략어인 webmitm이라는 Dsniff의 다른 또 하나의 프로그람을 기동시킨다. 이 도구는 전문적으로 SSL중계만 실행한다.
2. 공격자는 피해자콤퓨터에서 DNS질문신호가 오는가를 감시하다가 신호가 오면 가짜DNS응답신호를 보낸다. 이 가짜DNS응답신호에는 공격자콤퓨터의 IP주소가 들어 있다.
3. 피해자콤퓨터는 이 DNS응답신호를 받고 그 응답신호에 담겨 진 IP주소로 SSL대화조종을 개시한다.
4. 공격자의 콤퓨터에서 동작하고 있는 webmitm도구는 피해자콤퓨터와는 SSL대화조종을 실현하며 의뢰기와 실지 Web봉사기와의 다른 하나의 SSL대화조종도 실현한다.
5. 피해자는 SSL회선으로 자료를 보낸다. 피해자로부터의 SSL회선을 통해 오는 전송자료를 webmitm도구가 복호화했다가 다시 그 자료를 암호화하여 Web봉사기에

넘긴다. 중간에서 가로채 본것도 모르고 이 외부 Web봉사기는 전송자료를 받는다.

이 수법의 효력이 상당한것만은 틀림 없지만 공격자의 견지에서 볼 때는 한가지 제한성이 있다. 피해자와 공격자사이에 SSL련계를 지을 때 공격자는 자기의 SSL수자식인증서를 보내지 않으면 안되게 된다. 피해자가 보낸 모든 자료를 복호화하기 위해서도 실지 자료전송목표인 Web봉사기의 인증서가 아니라 자기 수자식인증서를 사용해야 한다. 피해자의 Web열람기가 공격자가 보낸 가짜인증서를 받으면 이 Web열람기는 사용자에게 경고문을 현시할것이다. 이 열람기는 봉사기에서 받은 인증서가 열람기가 신임하지 않는 인증기관의 서명을 받은것이라는 내용을 통보할수 있다. 그다음 열람기는 련결을 짓겠는가에 대한 사항을《OK》 혹은 《Connect》라는 단추를 제시하면서 사용자에게 묻는다. 대부분의 사용자들은 열람기의 이 경고문을 리해하지 못하고 성급히 련계를 짓는다. 열람기는 사용자가 그 가짜인증서를 접수하라고 하였으므로 안전한 결선을 한다. 결선이 된후 공격자는 SSL대화과정의 모든 자료를 손에 쥐게 될것이다. 본질상 공격자가 SSL인증서에 대한 신임결정을 사용자의 손에 맡기는셈이다.

명령쉘로 원격접속하는데 쓰이는 안전쉘(SSH)에 대한 공격에도 우와 꼭 같은 기법이 리용된다. Dsniff에는 SSH중간공격에 리용되는 sshmitm이라는 도구도 있다. SSL공격에서와 마찬가지로 Dsniff는 두가지 SSH접속을 실현한다. 하나는 피해자와 공격자사이이고 다른 하나는 공격자와 목적지봉사기이다. 여기서도 Web열람기는 조작된 SSL인증서에 대해 경고문을 내보내는데 SSH의뢰기는 SSH봉사기가 쓰는 공개열쇠를 왜 이 열람기가 인정안하는지 모르겠다고 두덜거린 다음 경고를 무시하고 련결시키면 SSH대화교환이 시작되며 이때에는 벌써 공격자가 모든 통신내용을 다 보고 있을 때이다.

적극적엿보기수법들에 대처한 방안들 공격자가 엿보기도구로 망우에서 오가는 유용한 정보를 몽땅 훔쳐 보는 조건에서 이러한 공격에 어떤 방도로 대처할것인가. 첫째로 망으로 교환되는 자료는 가능한껏 암호화해야 한다. Web통신에는 SSL, 암호화된 접속개시와 파일전송에는 SSH, 암호화된 전자우편에는 S/MIME, 망층암호화에는 IPSec 등 안전한 규약을 써야 한다. 사용자들은 기술적으로나 정신적으로나 각성하여 이러한 도구를 활용함으로써 기밀자료를 잘 보호해야 한다.

특별히 중요한것은 체계운영자들, 망관리자들, 보안담당자들이 이러한 안전규약을 리해하고 응용하여 자기 사업을 잘 수행하는것이다. 방화벽, 경로기, 기밀적인 봉사기나 공개열쇠기반체계에는 절대로 텔네트로 접속하지 말아야 한다. 텔네트가 이 경우 평문으로 송신하기때문에 공격자가 중간에서 통과암호를 가로채기가 너무나도 쉽다. 또한 열람기와 SSH의뢰기가 내보내는 경고문들에 특별히 관심을 돌려야 한다. 불확정한 인증서로 SSL대화를 개시하여 망으로 기밀정보를 보내는 현상이 없도록 하여야 한다. 만일 SSH의뢰기가 봉사기의 공개열쇠가 이상하게도 변경되였다고 경고문을 내보내면 수사해 볼 필요가 있다.

또한 집선기가 도중에서 정보가로채기에 걸릴수 있는 우려가 많으므로 집선기들을 없애는것도 고려해 볼 필요가 있다. 집선기보다 가격이 비싸지만 교환기는 보안신뢰도도 향상시키고 성능도 향상시킨다. 망에 교환기를 전반적으로 설치하는것이 불가능하다면 최소한 주요망경간에만이라도 교환대가 설치된 이써네트인 《비무장지대》(DMZ)를 구축

하는것도 방도의 하나라고 할수 있을것이다.

마지막으로 기밀체계와 기밀자료를 다루는 망들에는 교환기에 포구준위의 보안대책이라도 세워 놓아야 한다. 즉 매 교환기포구와 그 포구를 쓰는 기계의 고유 MAC주소를 설정하여 MAC주소범람문제나 가짜ARP통보문을 막아 낼수 있을것이다. 더 나아가서 인터네트 DMZ와 같은 기밀성이 높은 망들에서는 매 말단기계에서 LAN상의 모든 콤퓨터체계의 MAC주소들을 하드웨어적으로 코드화한 정적인 ARP표를 사용해야 한다. 교환기상의 포구안전체계와 하드웨어적으로 코드화한 ARP표들은 조작하기 매우 어렵다. 그것은 부품이나 지어 이써네트기판들을 교체하자면 여러 체계에 내장된 MAC주소들을 갱신해야 하기때문이다. 인터네트 DMZ 같은 매우 기밀적인 망들의 보안을 위해서는 이러한 준위의 보안대책이 필요하며 또 반드시 실행되여야 한다.

핵심부준위의 루트키트의 확산

공격자들은 ARP와 DNS와 같은 매우 중요한 기본규약들을 공격대상으로 삼고 있을뿐아니라 조작체계(OS)의 심장부도 남김없이 리용하고 있다. 특히 핵심부준위의 루트키트에 대한 개발이 상당한 정도로 진행되고 있다. 핵심부준위의 루트키트에 대한 리해를 보다 깊이 하기 위하여서는 그 개발과정의 조상이라고 할수 있는 전통적인 루트키트를 우선 분석해 보는것이 필요하다.

전통적인 루트키트

전통적인 루트키트는 공격자로 하여금 어떤 체계에 운용관리자(superuser)준위의 접근을 유지하게 하는 도구들의 묶음이다. 일단 공격자가 뿌리준위에서 어느 한 콤퓨터에 대한 조종을 실현하면 루트키트는 그 콤퓨터에 대한 접근을 지속하게 한다. 전통적인 루트키트에는 대체로 공격자가 정상보안조종체계를 우회하여 그 콤퓨터에 대한 접근을 할수 있게 하는 《뒤문치기》라는 도구도 있다. 루트키트에는 또한 공격자가 그 콤퓨터에 은거할수 있게 하는 각이한 프로그람도 있다. 기능이 가장 완비된 일부 루트키트로는 쏠라리스와 Linux에서 실행가능한 Linux루트키트 5(1rk5)와 T0rnkit가 있다. 다른것들과 마찬가지로 이 두가지 루트키트들은 http://packetstorm.security.com/UNIX/penetration/rootkits주소에서 구입할수 있다.

전통적인 루트키트들은 조작체계에 있는 주요실행프로그람들을 바꿔 치는 방법으로 뒤문치기수법과 은거수법을 실현한다. 실례로 대부분의 전통적인 루트키트프로그람들에는 /bin/login 프로그람을 바꿔 넣을수 있는 대체본이 있다. 이 /bin/login프로그람들은 사용자들이 UNIX체계에 접속할 때 인증용으로 쓰는 프로그람이다. 루트키트에 있는 /bin/login대체본은 공격자가 알고 있는 통과암호를 가지고 있어 이것으로 콤퓨터에 대한 뿌리준위의 접근을 할수 있다. 공격자는 공격대상인 콤퓨터에 있는 이전판 /bin/login에

루트키트의 대체본을 덧쓰기하고는 시간기록과 파일크기를 이전의것과 일치하게 조작한다.

/bin/login프로그람을 바꾸어 넣어 뒤문치기수법을 리용하는것처럼 대부분의 루트키트에는 체계관리자들이 체계분석에 쓰는 기타 UNIX용도구대용 트로이목마대체프로그람들도 있다. 많은 전통루트키트들은 1s명령문(흔히 폴더내용을 보여줌)대신 트로이목마대체본들을 쓴다. 변경된 1s명령문은 공격자의 도구들을 감추어 주어 절대로 현시되지 않게 한다. 또한 공격자들은 사용중인 TCP와 UDP포구들을 보여 주는 도구인 netstat프로그람을 자기의 대체본으로 바꾸어 공격자가 사용하는 포구들에 대해 거짓말을 하게 한다. 이와 류사한 방법으로 ifconfig, du, ps 같은 기타 많은 체계프로그람들도 바꾸어 치울수 있다. 이 모든 프로그람들은 체계관리자에게 있어서 눈과 귀의 역할을 하는것들이다. 공격자는 전통적인 루트키트를 사용하여 이 눈과 귀를 다 바꾸어 놓음으로써 체계에 공격자의 프로그람들이 존재하고 있음을 모르게 한다.

전통적인 루트키트들을 탐지하기 위해서 많은 체계관리자들은 《존경 받을만한》프로그람인 Tripware(http://www.tripware.com에서 구입가능함)와 같은 파일체계무결성검사도구들을 리용한다. 이 도구들은 사활적인 역할을 하는 체계파일(례하면 /bin/login,1s netstat, ifconfig, du, ps 등)에 있는 암호학적으로 강력한 하쉬들을 계산하여 이 수자식지문들을 쓰기방지한 플로피디스크와 같은 안전한 매체에 보관한다. 그다음 정기적으로(매체를 매일 혹은 매주마다) 무결성검사프로그람을 기동시켜 그 콤퓨터의 실행파일들의 하쉬를 다시 계산하여 따로 보관된 값과 비교한다. 변화가 있으면 그 프로그람을 수정하며 따라서 체계관리자는 각성을 높이게 된다.

핵심부준위루트키트

전통적인 루트키트들을 사용하여 사활적인 체계실행파일들을 바꾸어 놓는 한편 공격자들은 한걸음 더 나아가 핵심부준위루트키트들을 리용하고 있다. 핵심부란 디스크, 체계처리장치, 주기억 등과 같은 모든 자원의 접근을 조종하는 모든 OS의 심장을 말한다. 핵심부준위루트키트들은 응용프로그람준위의 파일들을 다치는것이 아니라 바로 그 핵심들을 변경시킨다. 그림 3－4의 왼쪽에서 보는바와 같이 트립와이어 같은 파일체계검사도구들은 핵심부에 기초하여 응용프로그람의 무결성을 검사하기때문에 핵심부를 다치지 않는 전통적인 루트키트들은 발견해 낼수 있다. 응용프로그람이 변경되면 좋은 트립와이어프로그람 같은것은 그 좋은 핵심부를 리용하여 트로이목마대체본프로그람들을 발견할수 있다.

그림 3－4에서 오른쪽에 있는것이 핵심부준위루트키트이다. 모든 응용프로그람들은 그대로 있지만 핵심부는 《썩어》서 공격자에게 뒤문도 열어 놓고 있으며 공격자의 체계침입에 대해서도 체계관리자에게 허위보고한다. 가장 강력한 일부 핵심부준위루트키트들로는 http://packetstorm.security.com/UNIX/penetration/rootkits에서 구입할수 있는 LINUX용 Knark, http://www.inforwar.co.uk/the/slkm–1.0.html에서 구입할수 있는 Plasmoid의 Solaris용 핵심부준위루트키트 그리고 http://www.rootkits.com에서 구입할수 있는 Windows NT용핵심부준위루트키트를 들수 있다.

전통적인 루트키트가 침해한 체계

핵심부준위 루트키트가 침해한 체계

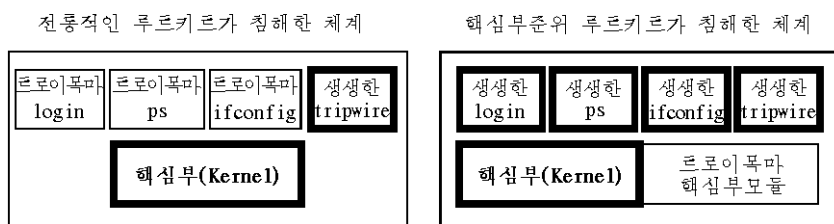



그림 3—4. 전통적인 루트키트와 핵심부준위루트키트

수많은 기능들을 가진 각이한 핵심부준위루트키트들이 현재 출현하고 있는 조건에서 그중 가장 인기 있는 기능들은 다음과 같이 묶어 볼수 있다.

- **실행방향바꾸기기능** 이 기능으로는 그 어떤 응용프로그람을 실행시키라는 명령을 중간에서 가로채여 그 명령을 조작하여 공격자가 선택한 다른 응용프로그람을 실행시킨다. UNIX의 /bin/login루틴과 관련한 씨나리오를 가상해 보자. 공격자가 핵심부준위루트키트를 설치한 다음 /bin/login파일은 고치지 않고 그대로 둔다. /bin/login이라는 모든 실행명령(누구든지 체계에 접속할 때마다 생기는 명령)은 조작되여 숨겨 져 있는 파일인 /bin/backdoorlogin을 실행시키게끔 설정된다. 어떤 사용자가 접속하면 뒤문치기통과암호도 있는 /bin/backdoorlogin이 실행되여 뿌리준위에 접근의 길이 열린다. 그러나 체계관리자가 트립와이어 같은 파일체계검사프로그람을 실행시키면 표준/bin/login루틴이 해석된다. 실행대상만 바뀐것이다. 원래의 /bin/login파일을 보고 그 무결성을 확인한다. 이 원래의 루틴은 변형되지 않고 있으며 트립와이어의 하쉬도 그대로 있다.
- **파일숨기기기능** 많은 핵심부루트키트들을 써서 공격자들은 파일체계에 그 어떤 파일도 숨기기를 한다. 그 어떤 사용자나 응용프로그람이 그 파일을 찾으면 핵심부는 그 파일이 존재하지 않는다고 거짓말을 한다. 물론 그 파일은 그 콤퓨터에 있으며 공격자가 마음 먹으면 언제든지 그 파일에 접근할수 있다.
- **과정숨기기** 파일을 숨기는것이외에도 공격자는 핵심부준위루트키트를 써서 그 콤퓨터에서 실행과정을 숨길수 있다.

이 매 특성들은 그자체로만도 그 기능이 상당히 강하다. 이것들을 합쳐 리용하면 공격자는 마음 먹는대로 그 콤퓨터를 완전히 개조할수 있는 능력을 가질수 있다. 체계관리자는 모든것이 그대로 있는듯하나 공격자가 《창조》해 놓은 체계를 보게 될것이다. 그러나 체계는 말그대로 속까지 푹 《썩은》것이다. 게다가 모든 체계접근이 공격자가 조작해 놓은 핵심부에 의존하므로 사용자가 핵심부준위루트키트유무검사를 해도 발견하기가 상당히 힘들다.

핵심부준위루트키트에 대처한 방안들 공격자들이 핵심부준위루트키트(혹은 전통적인 루트키트)를 설치하지 못하게 하기 위해서는 무엇보다먼저 공격자들이 우리 체계에 운용

관리자의 권한을 가지지 못하게 하는것이 중요하다(운용관리자란 임의의 파일에 자유롭게 접근할수 있을뿐아니라 콤퓨터체계의 운영과 사용, 보수 및 점검에 필요한 작업을 수행할수 있는 사용능력과 자격을 갖춘 관리자를 말한다–역주). 운용관리자로서의 권한을 주지 않으면 공격자는 핵심부준위루트키트를 설치할수 없다. 또한 중요한것은 체계설정을 안전하게 해놓아 모든 불필요한 봉사항목들은 제거하며 해당한 보강대책도 세워야 한다. 각 체계를 강화하고 체계들을 정비보강하는 사업을 정상적으로 하는것이 핵심부준위루트키트를 처리할수 있는 최선의 예방책이다.

또 하나의 방비대책으로서는 핵심부를 동적으로 수정시키는 일부 조작체계들의 기능인 적재가능핵심부모듈(LKM)을 지원하지 않는 핵심부들을 배치하는것이다. LKM들은 핵심부준위루트키트들을 실행시키는데 흔히 리용된다. LINUX핵심부들은 핵심부모듈지원이 없이 구성될수 있다. 그러나 쏠라리스 8과 그이상의 체계들은 핵심부모듈기능억제능력이 없다. 인터네트는 Web봉사기, 우편봉사기, DNS봉사기, FTP봉사기와 같은 사활적인 LINUX체계들에 대해서는 LKM접수능력 없는 자기체계의 핵심부들을 가지고 있어야 할것이다. 바로 비모듈적핵심부들을 가짐으로써만 다양한 형태와 수법의 공격을 물리칠수 있을것이다.

결 론

콤퓨터방위자들과 콤퓨터침공자들사이의 군비경쟁의 가속화는 계속 진행되고 있다. 침공자들이 광범한 분산공격수법을 개발하여 우리의 규약들과 조작체계들의 속으로 더욱 깊숙이 뚫고 들어 오는 조건에서 우리는 더욱더 열심히 일하여 우리 체계들의 안전을 지켜야 한다. 용기를 잃지 말라. 사실 이 장에서 언급된 방어기법들을 활용하자면 작업량이 적지 않다. 그러나 체계설계와 유지를 깐깐히 해나가면 틀림없이 안전한 기반을 구축할수 있을것이다.

제4장. 사회공학의 위험

죤 버티
마커스 로져스

정보보안실행자들은 정보기술의 주요목적이 사용성, 무결성, 비밀성(AIC의 3자일체)이라는데 대하여 너무나도 잘 알고 있다. 그러나 방어체계 혹은 보안체계안에 약한 고리가 하나 있다면 이 세가지 목적중 어느 하나도 달성할수 없다. 흔히 사람들이 말하는것처럼 정보보안에서는 가장 약한 고리가 어느 정도인가에 따라 보안강도를 판정할수 있다. 정보보안과 정보기술보안에 대하여 말할 때 우리는 흔히 이 보안체계의 련쇄고리들중 그 어떤 기술적분야만 생각하군 한다. 최신판조작체계와 응용체계나 하드웨어가 가지고 있는 취약점들을 서술한 수많은 참고도서들을 정보보안관리실행자들은 읽어 볼수 있을것이다. 많은 회사들도 이러한 취약점들을 먼저 발견하며 그에 기초하여 자기들의 기업경영계획들을 세우고 경쟁력을 키우며 그다음에야 사회와 판매업체에 대응책들을 제공하고 있다. 보안산업의 초점이 일차적으로 하드웨어, 쏘프트웨어, 펌웨어와 정보보안의 기술적측면들에 돌려 지고 있는것은 너무나도 명백하다.

보안산업은 콤퓨터들과 기술이 단순한 도구들이며 이 도구들을 사용하고 설정하고 설치하고 실행시키거나 악용하는것도 바로 사람이라는것을 잊어 버린것 같다. 정보보안은 단순히 여러가지 기술적인 복합조종과정을 실행하는것만이 아니다. 정보보안은 사람들의 행위, 더 정확히 말하여 비행을 처리하는 문제도 포괄한다. 정보보안이 효과적인것으로 되자면 《사람》을 나타내는 용어인 《웰웨어》(wetware)가 가지고 있는 약한 고리들도 극복하지 않으면 안된다. 숱한 자금과 노력을 들여 기술적통제수단들을 꾸려 놓고 더 좋고 더 안전한 코드를 만들어 놓았다 해도 우리 사람들이 《왕국으로 가는 이 열쇠들》을 루설해 버리면 이 모든 공사는 허사로 되고 말것이다. 망공격과 관련한 최근 연구자료들을 보면 이것들은 정확히 말하여 사람들이 무의식적으로 한것이라는것이다. 그렇기때문에 우리는 《사회공학》이라고 하는 공격으로 우리의 체계에 비법접근하는 량심 없는자들의 희생물이 될수 있는 가능성이 그만큼 더 높다.

이 장에서는 이러한 공격수법이 어떻게 진행되며 흔히 쓰이는 수법들은 어떤것들이며 또 교육과정과 강습, 통제로 사회공학의 위험성을 어떻게 약화시키겠는가 등을 자세히 해부해 봄으로써 사회공학을 일정하게나마 밝혀 보려고 한다. 이 장은 방도를 제시해 주는 장이 아니라 이러한 일부 공격수법들의 세부와 사회공학의 희생물로 되지 않기 위해서는 어떻게 할것인가를 토론해 보는 장이라고 볼수 있다. 이 모든 정보는 비밀이 아니며 사회의 일정한 분야들에 이미 널리 알려 진것들이다. 따라서 정보보안 전문가들도 사회공학과 그 위험성을 극복하기 위한 보안통제대책들에 대하여 잘 아는것이 중요하다.

사회공학의 정의

사회공학이란 무엇인가를 리해하자면 토론되는 내용이 무엇인가를 명백히 정의하는것이 우선 중요하다. 《사회공학》이라는 용어는 새로운 용어가 아니다. 사회조종분야에서 나온 용어이다. 사회공학은 일정한 목적의 결과를 얻기 위하여 어떤 하나의 협회(영어에서 a society는 《협회》나 《사회》를 의미함) 즉 더 정확히 말하여 공학자협회를 가리킬수도 있다. 이 용어는 또한 사람들이 일정한 새로운 체계나 체계에 복종시키기 위한 목적으로 그들의 행동을 예상대로 변화시키려는 과정을 가리킬수도 있다. 여기에서 적절한것은 바로 이 후자 즉 사회공학에 대한 사회심리학적정의라고 할수 있다. 우리의 목적의 견지에서

> 사회공학이란 《어떤 사람에게 영향을 주어 그가 정보를 류출시키게 하거나 정보체계, 정보망, 정보자료가 비법접근되거나 비법사용되거나 혹은 비법공개되도록 그 사람을 행동하게 하는 성공적 혹은 비성공적시도》라고 정의할수 있다.

정의에서 볼수 있는바와 같이 사회공학은 어떤 사람에 대한 속임수나 기만과 동의어적관계라고 할수 있다. 사람 한명쯤 기만하거나 깜짝 속이는것은 범죄활동의 령역에서는 아무런 새것도 아니다. 이 수법은 오래 존속되여 왔음에도 불구하고 아직도 놀라울 정도로 효력이 높다.

이 시점에서 사회공학이 안고 있는 문제점들의 규모가 얼마인지 일정한 정보를 알고 있다면 매우 흥미 있을것이다. 그러나 아쉽게도 여기에 쓸만한 자료는 거의 없다. 정보보안분야에서 사회공학에 대하여 자주 언급은 되였지만 이러한 형태의 공격에 대한 직접적인 토론은 지금까지 많이 진행되지 못하였다. 그 리유는 각이하다. 이 분야의 일부 사람들은 사회공학은 사람의 지능에 대한 공격이여서 그런 공격이 있었다는것을 사람들이 대체로 인정하려고도 하지 않는다고 말한다. 그러나 이에는 상관없이 일부 악명 높은 콤퓨터범죄자들은 실지 기술적문제보다 사회공학에 더욱 의거하여 자기들의 범죄를 계속하고 있다. 통과암호만 누구한테 물어 보면 되겠는데 무엇때문에 고생스레 시간을 랑비하며 남의 체계를 연구하고 스캔하며 체포될 위험까지 무릅쓰는가.

거의 모든 콤퓨터범죄자들은 다 기회를 노리는 기회주의자들이다. 그들은 남의 체계에로 들어 가는 더 쉬운 길을 노리고 있다.

어떻게 되여 사회공학이 작용하는가

사회공학적공격이 성공하는것은 주로 두가지 요인 즉 인간의 마음과 기업환경이다.

인간의 마음

사회공학적공격의 희생물이 되는것은 지능과는 아무런 관계도 없으며 인간적인것 즉

다소 순진하여 이러한 공격에 대처할만한 마음의 준비나 훈련이 부족한것과 전적으로 관련되여 있다. 사람들은 대개 본태적으로 남을 믿으며 남을 도와 주려고 하는것이다. 사회심리학은 인간관계를 집단과 개인의 견지에서 연구하여 왔다. 그 연구결과들을 보면 대체로 그 누구든 적절한 조건에서 재간 있는 사람과 교제를 하는 경우 영향을 받아 다른 환경에서는 루설하지 않을 정보도 루설하거나 류다르게 행동할수 있다고 한다. 또한 연구자료에 의하면 권력자이거나 권력자행세를 하는 사람들은 쉽게 다른 사람들을 위협할수 있다.

많은 경우 사회공학은 1차적인 목표물들이 문의소일군, 행정 및 기술지원일군들이므로 집단심리에 대치되는 개념인 개인심리를 리용하고 있다.

대인관계는 대체로 일대 일이나 서로 얼굴을 마주하는것이 아니다. 전화나 직결상태의 관계이다. 아래 부분에서 설명되겠지만 공격자들은 이러한 심리적인 공격에 약해 보이는 사람들을 항상 찾고 있다.

기업환경

기업병합과 흡수, 기술의 급속한 발전, 광지역망의 확산이라는 최근의 경영추세와 기업환경은 인간의 심리와 더불어 사회공학에 더 좋은 기회를 주고 있다. 오늘날의 기업세계에서 공급자, 판매자, 고객들은 제쳐 놓고서라도 자기 기관에서 항상 함께 거래하는 사람들을 한번도 만나보지 못했다는것은 틀린 말은 아니다. 종업원들을 위한 원거리통신체계와 기술이 너무나도 많이 도입되여 사람들사이에 일대 일로 얼굴을 마주 보며 하는 대인관계가 점점 더 희귀한 현상으로 되여 가고 있다. 오늘날의 시장세계에서는 어느 기관이나 기업을 위해 일한다 해도 몇몇 례외적인 사람들을 제외하고는 거의 사무실에 발을 들여 놓는 경우가 점점 희미해 지고 있다. 우리가 일하는 환경에서 흔히 있는 보지 못하고 진행되는 추상적인 대인관계에도 불구하고 사람들에 대한 근본적믿음 지어는 실지 한번도 만나보지 못한 사람들에 대한 이러한 믿음은 아직도 변함이 크게 없이 그대로인것이다.

오늘날 기업들과 기관들도 이전보다 훨씬 봉사지향적인 방향으로 나아가고 있다. 종업원들에 대한 평가는 흔히 그들이 협동적인 환경들에 얼마나 기여하였는가 그리고 고객들과 다른 부서에 대한 봉사수준에 따라 진행되군 한다. 그러나 자기 사업을 수행할 때 어느 정도의 상식을 리용하였으며 보안의식이 얼마나 있는가를 계측하는 평가지표들은 보기 힘들다. 사회공학의 위험에 효과적으로 대응하기 위해서는 바로 이러한 구조관계를 개선해야 할 필요가 있다.

사회공학적공격

사회공학적공격은 단계별로 진행되군 하는데 대부분의 경우 첩보기관에서 자기가 노리는 대상물에 침투하는 방법과 매우 류사하다.

간단히 보여 주기 위하여 그 단계들을 다음과 같이 묶어 볼수 있다.

- 정보수집
- 대상선정
- 공격

정보수집

사회공학적공격이 성과를 거두는 비결의 하나는 정보이다. 회사종업원으로, 판매업체 대표로 혹은 법기관의 성원으로 가장하기 위하여 어떤 기관이나 그 성원들에 대한 충분한 정보를 쥐는것은 상당히 쉽다. 각 기관들에서는 자기들의 시장경쟁력을 높이기 위한 전략의 한 고리로서 Web싸이트에 너무나도 많은 정보들을 내놓고 있다. 이 정보들을 보면 대개 어떤 판매업체와 대상하고 있는가 하는 단서들, 전화번호와 전자우편목록들도 있으며 지사들이 있는가 없으면 어디에 있는가 하는 내용들도 다 알수 있게 되여 있다. 일부 기관들은 지어 자기들의 Web페지들에 자기 기관의 조직구성도를 구체적으로 그려 내놓기까지 하고 있다. 투자를 희망하는 사람들에게 이 모든 정보가 유용할수 있으나 이것은 사회공학적공격에도 하나의 중요한 발판으로 리용될수 있다.

깊이 생각하지 않고 만들어 낸 Web싸이트들만이 공개정보의 원천으로 되는것이 아니다. 기관들에서 버린것들도 중요한 정보원천으로 될수 있다. 해당 기관의 쓰레기장을 쭉 지나가면(이것을 쓰레기장산보라고도 한다.) 공격자가 중요한 정보를 장악하는데서 도움이 될수 있는 송장들, 서신들, 사용지도서 등이 많이 보인다. 법에 기소된 여러 콤퓨터범죄자들은 대상물에 대한 정보를 수집하기 위하여 쓰레기장산보를 했다는것을 실토하였다.

이 단계에서 공격자의 목적은 될수록 많은 정보를 알아냄으로써 자기를 합법적인 진짜직원, 계약자, 판매자, 전략적동반자 혹은 경우에 따라 법기관 혹은 수사기관일군으로 가장하는것이다.

대상선정

일단 충분한 량의 정보를 수집하면 공격자는 그 기관의 성원들중에서 눈에 띄우리만큼 약한 고리들을 찾는다. 가장 흔히 선택하는 대상은 문의소(helpdesk)일군들이다. 그것은 이들이 문의방조를 줄수 있게끔 강습 받은 전문가들로서 통과암호변경, 사용자기록부 창조 및 재개 등을 맡아 처리하기때문이다. 일부 기관들에서는 그들의 봉사기능을 계약에 의해서 실지 거래관계가 없는 제3자에게로 확대하기도 한다. 이것은 계약을 맺은 제3자기관이 이 기관의 종업원들을 한명도 모를수 있음으로 하여 사회공학적공격의 성공의 기회는 더욱 좋아 진다. 공격자들은 이 경우 기밀정보수집이나 체계에로의 발판확보에 목표를 두군 한다. 공격자들은 고객수준에서라도 접근이 허용된 이상 고객으로서 봉사받을 특권을 더 높여 보다 파괴적인 공격을 실행하며 자기들의 흔적을 지울수 있는 가능성이 상대적으로 높다고 본다.

행정관리일군들의 보조자들이 그다음으로 가장 많이 선정되는 피해자들이다. 그 리유는 주로 경영측의 고위일군들사이에만 오고가는 다량의 기밀정보들에 접촉하는 사람들이 바로 이들이기때문일것이다. 이들은 공격대상점으로 리용되든가 아니면 그 기관내의 영향력 있는 인물들의 이름과 관련한 보충정보수집에 리용되는것이 상례이다. 그 기관에서 모든 일을 《쥐락펴락하는 사람》들의 이름을 알면 필요할 때 《거 아무개 있잖아》 하는 식으로 자기 친구이름 부르듯이 하여 자기를 과시할수도 있을것이다. 또한 많은 행정일군보조자들이 자기 집행리사의 통과암호들을 알고 있으면 더욱 좋을것이다. 이 많은 보조자들은 정상적으로 자기 회사들의 구좌특혜에 관한 계산작업(례하면 계산표갱신)과 전자력서로 면담약속 등을 계획하는 등 여러가지 일을 한다.

공 격 수 법

실제적인 공격은 흔히 con이라고 부르는 수법들에 기초한다(여기서 con이라는 단어는 사람들의 신임을 상당히 얻은 다음 그것을 발판으로 그들에 대한 사기행위를 하는 자들 즉 confidence artist들을 간단히 부르는 말이다.–역주). 이것들을 부류별로 묶어 보면 세가지 즉 (1) 대상의 허영심이나 자만심을 자극하는 방법의 공격형태들, (2) 동정심이나 공감을 교묘히 리용하는 공격형태들, (3) 협박에 의한 공격형태들로 갈라 볼수 있다.

자만심을 리용한 공격

첫번째 형태의 공격인 자만심이나 허영심을 리용한 공격에서는 공격자가 인간의 가장 기초적인 특성들을 몇가지 리용하게 된다. 우리모두는 다른 사람들이 우리들을 보고 상당히 똑똑하다고 말하면 좋아 하며 자기가 하는 일에 대하여 그리고 회사사업이 제대로 되자면 어떻게 해야 하는가에 대해서는 실지로 알고 있다. 공격자들은 이것을 리용하여 만만한 사람들이 자기 지식을 굉장히 과시할 때 긍정해서 들어 주는 식으로 필요한 정보를 얻어 낸다. 공격자는 응당한 평가를 받지 못하고 있다고 느끼는 사람들과 가지고 있는 재능에 비해 낮은 지위에서 일하는 사람들을 공격대상으로 선정한다. 공격자가 이런것을 알자면 그러한 사람들과의 대화를 간단히 한번 하면 되는것이다. 흔히 공격자들은 이런 공격수법을 리용하여 정확한 대상을 찾을 때까지 서로 각이한 여러 사람들과 만나 이야기한다. 불행하게도 대부분의 경우 피해자는 자기가 무엇을 잘못했다는것을 전혀 모르는것이다.

동정심을 리용한 공격

두번째 부류의 공격에서 공격자는 흔히 자신을 새로 들어 온 동료사원, 계약자 혹은 어느 판매업체의 신입사원으로 가장하고는 우연히 곤경에 빠져 있는데 급히 무슨 일을 처리하기 위해 방조가 필요한듯이 말한다. 여기서 바로 첩보단계의 중요성이 명백히 나

타나는데 그것은 공격자가 그 만만한 사람에게서 일정한 정도의 신임을 얻어 그 사람이 공격자의 신원에 대해 그대로 믿도록 해야 하기때문이다. 이렇게 하자면 권위 있는 최고 실력자들의 이름들을 마치도 자기 동무들의 이름을 부르듯 하며 그들이 사용하는 적당한 은어들과 낱말들도 입에 올리며 그 기관에 대한 자기 지식도 보여 주어야 한다. 그러면서 자기는 바빠서 자료를 좀 봐야 할 일이 있는데 구좌이름이나 통과암호가 생각나지 않는다는것, 실수로 열쇠를 방에 놓은 채 문을 닫고 나와서 그런다고 꾸며 댄다. 여기서 매우 급해서 그런다는 내용이 중요하다. 그것은 그래야 필요한 절차들을 건너 뛰여 공격자가 《진짜인물》로 되며 자료에 접근할수 있기때문이다. 공격자가 가장한 그 인물의 감정에 동정을 표시하는것은 인간의 일반적인 심리이다. 결국 대부분의 경우에 이 요구들은 수락되게 된다. 공격자는 어느 한 사원으로부터 정보나 정보접근을 얻지 못하는 경우 동정하는 사람을 찾을 때까지 혹은 그 기관전체가 자기를 의심한다는것을 깨달을 때까지 계속 더 공격을 시도할것이다.

협박을 리용한 공격

세번째 부류의 공격에서는 공격자가 자신을 권력인물로 즉 그 기관의 유력자나 혹은 문건관계에서는 법기관인물로 가장한다. 공격자는 자기가 가장한 인물의 지위보다 몇단계 낮은 위치에 있는 만만한 사람을 목표로 한다. 공격자는 그럴듯한 구실을 하나 꾸며 통과암호재설정, 구좌변경, 콤퓨터체계접근권 혹은 기밀정보를 일정한 형태로 요구한다(기밀정보의 경우 법기관일군으로 가장하며 이때에는 《극비》조사라느니 국가안전과 관련한 문제라거니 하는 씨나리오를 연출하여 그 사원이 이 사건을 더는 들고 다니지 못하게 한다.》. 공격자는 자기가 마치도 그 사람에게 으름장을 놓을수는 있으나 잘 알려 질 정도의 인물은 되지 못하는척 한다(최고행정관 즉 회사사장이나 리사장들은 보도매체나 년례종업원총회에서 잘 알려 진 인물이며 대부분 업무시간이 지난후에 자기 종업원들을 찾아 잊어 버린 통과암호를 고치라고 요구할수는 없는것이다. 그런것들은 보좌성원들이 할 일이다.). 공격자들의 각본에서 기본은 시간이다. 그것은 공격절차가 어떠하든 우회할 필요가 있기때문이다. 만약 저항에 부딪치면 공격자는 너희들이 말 안들으면 제재를 받게 하겠다는 식으로 위협하여 협조해 나서도록 할것이다.

위험을 완화하는 방도

사회공학적공격의 형태가 어떠하든지 성공률은 놀랄만큼 높다. 기소된 콤퓨터범죄자들은 대부분 사람들이 자기들의 수에 간단히 속아 자기들의 체계에로 《걸어 들어 갈》수 있게 해준데 대해 롱담까지 하고 있다. 사회공학적공격의 위험성과 영향은 크다. 이러한 공격자들은 대개 추적하기 힘들며 일부 경우에는 누구인지 밝혀 내기 힘들다. 공격자가 만일 합법적인 접속기록철을 통하여 접근권을 얻었다면 경보신호는 절대로 울리지 않을것이다. 그것은 체계와 관련된 문제에서는 잘못한 점이 전혀 없기때문이다.

사회공학이 실현되기 쉽다면 각 기관들은 이런 공격의 위험성을 어떻게 방지할것인가. 이 문제에 대한 대답은 상대적으로 간단하다. 그러나 기관의 전체 성원들의 사고관점에서의 변화를 필요로 한다. 즉 사회공학의 위험성을 약화시키기 위해서는 각 기관들이 자기 종업원들속에서 정보보안상 위험성들과 사회공학적공격의 경우들을 발견해 낼수 있게 교양사업과 강습을 잘 진행해야 한다. 이러한 공격을 억제할수 있는 방도는 바로 교육하고 알려 주며 훈련시키는 등 여러가지 통제사업에 있다. 이에 대해서는 아래에서 보자.

사회공학의 대상은 정보보안이라는 련쇄고리에서 가장 약한 고리인 사람들에게 초점이 맞추어 져 있다. 어떤 사람이 한 사원을 설득시켜 기밀정보를 제공하게 할수 있다는 사실은 가장 안전한 체계에도 취약성이 있다는것을 의미한다. 그 어떤 정보보안해결책이든지 사람이 거기서 노는 역할이 가장 중요하다. 사실상 모든 정보보안해결책들은 사람이라는 요소에 많이 의거한다. 이것은 이 약한 고리인 사람이라는 요소는 하드웨어, 쏘프트웨어, 가동환경, 망, 설비로화 등과는 관계없이 보편적이라는것을 의미한다.

많은 회사들은 정보보안을 잘 담보하기 위해 수만딸라를 지출한다. 이 보안체계는 그 회사들이 정보까지 종합하여 자기의 가장 중요한 재산을 지키는데 리용된다. 불행하게도 이렇게 최상급으로 꾸려 놓은 보안체계도 사회공학적기법을 적용하는 경우 무효로 되여 버릴수 있다. 사회공학적기법들은 매우 원가가 눅으며 매우 낮은 기술수단들을 리용하여 이 정보보안대책들의 장애를 제거해 치운다.

사회공학에 대처한 보호

사회공학의 위협으로부터 자신들을 보호하기 위해서는 정보보안에 대한 초보적인 리해가 필요하다. 간단히 말하여 정보보안이란 정보에 대하여 우발적이든 의도적이든 비법적으로 로출시키거나 이전시키며 변경시키거나 파괴하는 현상을 미리 막는것이라고 정의할수 있다. 일반적으로 보면 정보보안은 한 회사의 자료와 정보, 체계와 봉사가 그 어떤 형태의 위협으로부터 정확히 보호될 때 그 회사가 도달한 상태를 의미한다. 정보보안은 다양한 형태의 위협으로부터 정보를 보호함으로써 기업의 존속을 담보하고 기업의 손실을 최소화하며 투자결과나 기업의 호기를 최대화하는것이다. 정보보안은 기업의 돈, 영상, 명예 그리고 그 기업의 존재를 안전하게 지키는 문제이다.

보호과정은 흔히 세가지 부류로 나눌수 있으며 여기서 중요하게 알아야 할것은 기관의 정보보안을 정확히 해나가자면 사회공학적공격을 비롯한 어떤 형태의 공격위협이든지 그로부터 자신을 정확히 지키기 위하여서는 이 세가지를 다 결합시키는것이 필수적이라는것이다.

- 물리적보안
- 론리적(기술적)보안
- 행정적보안

정보보안실행자들은 정보보안관리는 균형적으로 진행되여야 한다고 오래전부터 생각하여 왔다. 《균형적》이라는 말의 뜻은 회사마다 다르며 체계의 취약점들, 위험요소들, 정보의 기밀성을 의미하기도 하나 일반적으로 우에서 언급한 세가지 요소들을 다 가리키기도 한다. 정보보안의 대책적계획은 매 기업자체의 구체적실정과 요구에 맞게 작성되여야 한다. 정확한 균형을 달성한다는것은 이상의 세가지 부류에 다 맞는 여러가지 정보보안대책들을 다 강구하면서도 기관의 보안요구사항들을 가능한껏 효과적이며 원가가 적게 드는 방향에서 만족시킬수 있는 정확한 균형을 잡는다는것을 의미한다. 정보보안이 잘 되면 기관의 귀중한 정보재부를 찾아 내는 과정으로 되기도 한다. 즉 이 재부들에 대한 있을수 있는 위험의 범위를 고려하며 이 실태들에 대처한 효과적인 대책을 세우며 이 대책들이 정확히 계획되고 실행되고 납득되도록 하여야 한다.

물리적보안

물리적인 보안요소들은 가장 리해하기 쉬우면서 실행하기도 가장 쉽다고 한다. 물리적보안에 대하여 생각하면 많은 사람들의 머리에는 열쇠, 자물쇠, 경보기, 경비원들이 떠오를것이다. 이것들이 정보안전에 고려되는 유일한 보안대책들은 아니지만 바로 론리적으로 볼 때 여기가 출발점이라고 할수 있다. 론리적보안과 행정적보안과 함께 물리적보안은 정보보안대책안들중에서 사활적인 요소로 될뿐아니라 근본적인 문제로도 된다. 물리적보안이라고 할 때 이것은 정보자산을 도난, 파괴, 재난, 자연재해, 고의적 및 우발적사고 그리고 전기, 온도, 습기 등과 같은 불리한 환경적조건으로부터 보호하는것을 말한다. 물리적보안을 잘 유지하려면 훌륭한 건물 및 시설조건, 비상대응능력, 믿음직한 전원공급, 믿음직하고 정확한 온습도조절 그리고 내외의 침입자들로부터의 효과적인 보호가 필요하다.

론리적(기술적)보안

론리적보안대책들이란 기술적방안을 리용하여 정보재산을 지키는 대책들을 말한다. 실례로는 방화벽체계, 접근조종체계, 통과암호체계 그리고 침입탐지체계들을 들수 있다. 이 통제체계들은 매우 효력이 있으나 성과적인 보안대책으로 되자면 사람이라는 요소 혹은 인간호상관계에 대한 정확한 리해에 기초해야 한다. 우에서 언급한바와 같이 보다 쉽게 리용될수 있는것이 바로 이 사람이라는 요인이다.

행정적보안

행정적보안통제는 대책안, 절차, 지도서 등을 념두에 둔다. 행정적보안의 실례로는 정보보안방책안, 의식화계획 그리고 신입사원들을 위한 경력조사 등을 들수 있다. 이 실례들은 행정적성격을 띠므로 론리적 및 기술적실행대안으로는 되지 못하나 이 모든것들은 함께 정보보안문제를 제기하고 있다.

포 괄 범 위

정보보안이 효과적인것으로 되자면 우로부터 아래에 이르기까지, 지도일군들로부터 말단사용자에 이르는 기관전체가 다 망라되여야 한다. 가장 중요하게는 어느 기관이든 그 기관의 최고위층의 지도일군들이 정보보안과 관련한 구상과 원칙들을 승인하고 지원해야 한다. 꼭대기로부터 말단에 이르기까지 모든 사람들이 해당 보안방책들을 리해하고 그에 따라 행동하여야 한다. 이것은 고위관리일군들은 기관의 정보보안방책들을 규정하고 지지하고 내려 보내며 이것을 기관내 모든 사람들이 준수한다는것을 의미한다. 또한 이것은 웃단위일군들이 정보보안을 위하여 자금과 자원을 제공하는 등 필요한 지원을 준다는것도 포괄한다. 총괄적으로 볼 때 정보보안방책이 성과를 거두기 위해서는 웃단위일군들의 지도능력, 확고한 결심, 적극적인 참가가 절실히 필요하다.

결정적인 정보보안전략들이 제대로 실현되기 위한 조건은 1차적으로 모든 사람들이 절차대로 정확히 행동하는것이며 2차적으로는 기술적대책안들을 리용하는것이다. 그렇기때문에 사회공학이라는 위협에 대처해 나가는것이 모든 정보보안계획에서 결정적인 문제로 되는것이다.

사회공학적공격에 대처한 보안

방책작성, 의식화사업 및 교육

사회공학적공격들에 대처하기란 매우 힘들다. 사회공학적공격에 대처하는데서 문제로 되는것은 거의 모든 론리적보안통제의 보호기능이 무력하게 되는것이다. 사회공학적공격의 대상이 사람이기때문에 행정적측면의 정보보안에 보호대책의 초점이 놓여 져야 한다. 효과적인 대응책의 하나는 기관전반에 구현할수 있는 훌륭한 정보보안방책을 세워놓는것이다. 기관 종업원들의 《행동규범》을 작성하는데서 방책은 근본바탕으로 된다. 두번째 효과적인 대응책은 사용자에 대한 의식화 즉 교양사업을 잘하는것이다. 이 두가지 행정적인 정보보안대응책들을 잘 결합해 나가면 그것이 종합적인 정보보안계획으로 되여 모든 사람들이 그것을 자기들의 실지사업에서 지켜야 할 준칙의 하나로 리해하고 접수할것이다. 기관의 경영적견지에서 보면 이러한 내용을 우로부터 아래에 이르기까지 전체 종업원들에게 전달하는것은 사활적인것이 아닐수 없다. 결국 이렇게 되면 각급 부서들은 보다 경각성을 높이게 될것이며 각자가 모두 회사전체의 복리에 《기여》하게 될것이다. 이것은 회사종업원들모두가 만족스럽게 일해 나갈수 있게 하는데 크게 기여하는 중요한 하나의 관점이다. 이것은 또한 정보보안계획에서 또하나의 중요한 우려로 되는 종업원들의 불만이라는 위험성도 제거할수 있게 한다. 불만을 가진 이러한 종업원들이 바로 사회공학적방법은 어떠하든 기관내의 기밀정보들을 비법사용자들에게 쉽게 넘겨 주는 사람들인것이다.

사람들은 흔히 직접 체험해 보아야 가장 잘 알게 된다. 매 사람이 사회공학적공격을

당할수 있다는것이 증명된 이상 각자는 보다 각성을 높여 경계하게 된다. 다른 기관의 경험에 대한 토론연단 같은것을 조직하면 자기 기관사람들이 이러한 사회공학적공격에 더 큰 면역성을 가지게 할수도 있다.

교양사업을 꾸준히 진행하는것은 매우 중요하다. 교양과정을 정기적으로 반복하여 진행함으로써 사회공학과 관련한 기관의 방책들로 재무장시켜야 한다. 기술이 발전된 오늘의 조건에서 자기 기관의 종업원들과 정기적으로 만나 담화할수 있는 효과적인 방도를 세우는것은 매우 쉽다. 이러한 형태의 연단을 마련할수 있는 좋은 방도는 내부망Web싸이트를 리용하여 거기에 기관의 방책들은 물론 사회공학에 관한 재미 있는 이야기들과 이때 지켜야 할 안전사항과 안전정보를 담아 내놓는것이다. 사람들이 흔히 남의 불행한 일에 대해 듣기 좋아한다는 사실을 고려할 때 이러한 재미나는 이야기를 Web싸이트에 실으면 말하자는 내용의 요점이 더 널리 잘 전달될수 있을것이다.

《공적》에 대한 인정

때로 그 무슨 공적에 대하여 적극 인정해 주면 효과가 가장 클 때도 있다. 가령 한 종업원의 정보보안사건과 관련한 문제에서 잘 처리했다고 하면 그 모범적인 행동을 평가하고 그에게 응당한 표창도 주어야 한다. 그러나 거기에 머무르면 안된다. 기관내 다른 사람들모두가 이것을 다 알게 해야 한다. 그러면 결국에는 그 기관전체의 대응준비상태가 높아 질것이다.

사건대응팀의 준비

모든 회사들은 사건과 같은것에 효과적으로 대응할수 있는 능력을 가지고 있어야 한다. 사건이란 회사의 생활을 위협하는 그 어떤 일이 일어 나는것이라고 정의할수 있다. 정보보안의 견지에서 볼 때 외부적인 위협(사회공학까지 포함한)에 대처하는것이 곧 사건으로 된다. 잘 준비된 사고대응팀의 목적은 있을수 있는 정보보안위반현상들을 적발하며 회사에 줄수 있는 영향을 없애는 방향에서 사태를 효과적으로 대처해 나갈수 있는 방도를 제공하는것이다. 2차적이면서도 역시 매우 중요한 목적은 적절한 행동방향을 취할수 있는 충분한 정보를 경영측에 제기하는것이다. 사회공학적공격에 대처한 교육과 전습을 받을수 있는 회사의 주요부서들에서 뽑은 지식 있는 인재들로 구성된 팀을 가지는것은 효과적인 정보보안사업의 관건적측면의 하나이다.

준비상태에 대한 시험

침투시험을 진행하는것은 외부사람의 견지에서 기관의 보안대책들을 검열해 보는 하나의 방법이다. 좋기는 내부적침투와 외부적침투를 막거나 추적하며 경보신호를 내는 모

든 조치들을 다 시험해 보는것이다. 사회공학적공격에 대처한 준비상태를 검열해 보려는 회사들은 이 방법을 리용하여 이전에 발견할수 없었던 약한 고리들을 찾아 낼수 있다. 그러나 잊지 말아야 할것은 침투시험이 기관의 보안조치들을 평가해 낼수 있는 가장 좋은 방도의 하나이기는 하지만 그 시험을 집행하는 개별적사람들의 노력에 따라 그 효과가 좌우된다는것이다.

공격대상에 대한 즉시적인 통보체계

어떤 사람이 사회공학적시도에 대하여 보고하거나 발견하면 류사한 부문에 있는 모든 사람들에게 통지해 주어야 한다. 바로 이 단계에서 표준공정과 신속한 실현절차를 가지는것이 매우 중요하다. 바로 이 분야가 잘 준비된 사건대응팀이 나서서 도와 주어야 할 분야이다. 그러나 절차가 있다고 가정하면 사건대응팀은 재빨리 그 문제에 대처하여 손해가 오기전에 효과적으로 그 위험을 제거할수 있다.

필요한 곳에는 기술을 적용하라 종업원들에게 있을수 있는 위험성에 대해 알려 주며 또 정보를 요구하는 동료나 다른 사람들을 어떻게 대상해야 하는가에 대하여 지도해 주는것을 내놓고는 사회공학으로부터 정보와 종업원들을 보호해 주는 공고한 다른 방법이란 없다. 그러나 다음과 같은 몇가지 대안들도 고려해 볼 필요가 있다.

- **가능하면 통화를 추적하라** 통화추적은 할수도 있고 안할수도 있지만 추적능력이 있고 또 추적준비가 되면 할수 있다. 공격을 받는 도중에 《어떻게 통화를 추적한단 말인가》하고 생각하면서 망설이지 말아야 한다. 여기서도 마음의 준비가 있어야 한다. 사건대응절차가 있어 효과적으로 이에 대처할수 있어야 한다.
- **물리적보안상태를 잘 유지하라** 이미 언급된것처럼 보호체계를 잘 세우는데서 물리적보안을 잘 유지하는것은 필수적이다. 최신기술을 리용하여 자기의 자원을 믿음직하게 보호할수 있는 방도는 많다. 생체계측기술인 스마트카드를 리용하는 방법도 있다.
- **자료분류기준에 따라 기밀문서들을 표시하라** 정보분류기준을 잘 세워 놓으면 사회공학적공격이 있어도 기밀정보가 루설되는것을 막을수 있다. 실례로 그러한 공격에 넘어 가 어떤 문건을 꺼내다가도 그 문건에 쓰인 《비밀》이라는 표식을 보고 단념할수도 있다. 이와 근사하게 분류기준에 따라 파일을 전자적으로 표식해 놓아도 같은 효과를 기대할수 있다.

결 론

공격자가 리용하는 사회공학적방법들은 그 어느 기관이든 정보의 안전에 심각한 영향을 미친다. 이런 공격이 성공한 생동한 실례를 들자면 끝이 없다. 그러나 정보체계보안을 위한 일부 기초적인 원칙들을 준수하면 사회공학적공격의 위험성을 일정하게 약화시킬수 있다. 자기 기관에 맞게 방책을 잘 세워 극비 혹은 기밀로 되는 정보를 정확히 다루고 열람하는 지침서를 제시해 둘 필요가 있다. 정보보안관념도 매우 중요한 역할을 한다. 위험성들을 사람들이 다 알도록 하며 더 중요하게는 사건이 발생하는 경우 이에 어떻게 대응해야 하는가를 잘 알려 주어야 한다. 종업원들에게 정보보안의 중요성을 인식시키며 기밀정보를 손에 넣기 위해 자기들에게 접근하여 어째보려고 하는 자들이 있다는것을 알려 주는것은 벌써 방어의 현명한 첫 단계로 된다. 다만 있을수 있는 공격에 대하여 사람들에게 미리 경고해 두기만 해도 사람들은 경각성을 높여 그런 자들을 적발하고 해당 조치를 취할수 있을것이다. 옛말에 《지식은 힘이다.》라고 하였는데 이것은 사실이며 이 경우에는 보안을 더욱 강화해야 한다.

방화벽 같은 기술적으로 공고한 안전장치들을 해킹하는것보다 사람들을 해킹하는것이 훨씬 더 쉽다. 그러나 그 방화벽체계의 안전성을 잘 보장하는것보다 사람들을 교양하여 준비시켜 사회공학적시도들을 예방하고 색출해 내는것 역시 품이 훨씬 더 적게 든다. 모든 기관들은 이제 더는 사람들을 정보보안이라는 련쇄고리에서 가장 약한 고리로 보지 않을것이다.

제2편
원격통신과 망보안

망으로 련결되는 범위가 늘어남에 따라 콤퓨터사용은 상당히 광범해 지고 있다. 원거리통신기술로 하여 나라의 방방곡곡 그 어디에서나 세계 어느 지역, 어느 장소에서나 서로 정보를 신속히 주고받을수 있게 되였다. 이 제2편이 제일 방대한 부분으로 되는것은 그리 놀라운 일이 아니다. 그것은 이 부분이 정보통신기술의 보안과 나날이 확대되는 인트라네트, 인터네트, 엑스트라네트의 령역까지 포괄하고 있기때문이다.

한개 기관의 령역을 보호하는데서 계속 중요한 역할을 수행하는 방화벽은 이 부분에서 심도 있게 보기로 한다. 방화벽이란 본질상 두개의 망사이의 차단물로서 안으로 들어 오고 밖으로 나가는 모든 정보흐름을 다 검열하여 고정된 규정에 따라 그 전달을 허용하거나 거부한다. 이 부분에서는 려과장치들의 여러 측면들을 서로 비교해 보게 된다.

방화벽이 일정한 수준의 보호는 해주지만 기관의 정보(례하면 전자우편)는 그 기관안팎으로 흐르게 되여야 한다. 그런데 이 통신통로를 개방하게 되면 위태로운 현상이 일어 날수 있다. 이 부분에서는 정보의 자유로운 흐름이 가져 올수 있는 약점들과 이에 대처한 보호절차와 봉사형태들을 포괄하여 알려 주게 된다. 1980년대 후반기의 콤퓨터비루스는 오늘날 사처에 퍼져 있는 《장난질코드》에 비해 보면 유순한편이다. 정보통신망으로 온 세계가 뒤덮임으로 하여 무엇이든 신속히 복사할수 있게 되였다. 제조업체들이 내놓은 체계의 약점(혹은 기능)을 리용한 악명 높은 해킹프로그람들이 미칠듯한 속도로 인터네트를 종횡무진하고 있다. 회사들이 될수록 빨리 대응책들을 강구하고 있으나 내부기관들은 능력이나 도구가 부족하여 자기들의 기반을 미처 보강하지 못하고 있는 실정이다. 이 부분에서 볼수 있는바와 같이 일부 경우 대화식지원을 제공하는 소규모제조 및 판매업체들은 스팸과 악성비루스와 같은 위험사건들에 대처하기 위하여 내부적보안을 강화하는 사업에 봉사를 제공하기도 한다. 이 업체들은 또한 매주 7일간 매일 24시간의 감시체계도 제공하며 많은 경우 기관내적인 자원으로는 충당할수 없는 조기통지체계도 제공해 주고 있다.

망으로 통과하는 자료들을 보호할수 있는 가장 성공적인 방도의 하나는 가상개별망(VPN)에서 쓰이는 교갑화와 암호화의 사용이다. 이 부분에서는 자료의 안전을 유지하면서도 공공망을 통하여 개인정보를 주고받고 하는 가상개별망의 개념과 원리들을 구체적

으로 보게 된다. 대상들과 거래를 안전하게 가질수 있고 상품 및 물품조달을 위한 새로운 통로를 제공하며 눅은 원가로 새로운 시장에 접근할수 있는 좋은 점을 가지고 있는 외에도 이 VPN들은 커다란 잠재력을 가지고 있다. 이 부분에서는 VPN기술을 평가하고 도입하며 리용할수 있는 방도들과 이 기술에서 있을수 있는 약점들을 깊이 있게 파헤쳐 줄것이다.

콤퓨터기술과 통신기술이 급속히 발전하며 기구들이 소형화되고 있으면서도 동시에 기능화되여(소비자가 장소와 유선이나 무선에 관계없이 또 이동하면서도 봉사를 받을수 있는) 이동성(하드웨어나 쏘프트웨어의 구성요소가 쉽게 변경되고 확장될수 있는), 융통성(통신접속시간과 통신과정에 드는 시간을 빠르게 하여 주는), 신속성을 제공해 주고 있다.

이러한것들은 그 어느 다른 분야보다도 무선통신에서 더욱 그러하다. 특히 케블의 설치와 설정, 선로련결장치들이 필요 없는것으로 하여 무선통신망들은 더욱더 원가가 적게 들고 있다. 그 어떤 유선장치에 속박됨이 없이 정보접근을 실현하려는 지향은 기업운영의 필수적요구로 제기되고 있다. 그리고 아직 유선통신세계가 자체의 취약성을 가지고 있는것도 사실이다. 이 부분에서는 구내통신망과 인터네트상의 무선통신환경을 물리적층에서 어떻게 안전하게 구축하겠는가 하는 문제를 다루게 된다.

제5장. 보안과 망기술

크리스 해어

정보보안관계자들에게 있어서 망련결상태와 관련한 문제들을 점검하는것은 흔히 있는 일이기는 하지만 실지 망구성과 관련한 방법들과 기술에는 일정한 정도로 모르는 측면들도 있을수 있다. 이 장에서는 망이란 무엇이며 각이한 망구성방법에는 어떠한것들이 있는가를 보기로 한다. 또한 망보안을 둘러 싼 여러 문제점들도 소개한다.

사람들은 흔히 망을 통하여 육성, 영상, 음성 및 자료를 보낸다. 인터네트를 리용하여 은행거래를 하기도 한다. 직결상태에서 백과사전에서 필요한 정보를 검색하기도 한다. 친구들이나 가족들과 전자우편이나 영상전송을 통하여 련계를 가지기도 한다. 오늘날의 세계에서 전자수단을 통해 이렇듯 많은 정보가 교환되는 조건에서 정보보안실행자들이 오늘날의 콤퓨터망체계에서 사용되고 있는 망하드웨어의 기초들을 잘 아는것은 초보적인 문제라고 할수 있다.

망이란 무엇인가

망이란 정보교환을 위하여 둘 또는 그이상의 서로 련결된 기구들을 말한다. 망이라고 하면 사람들은 콤퓨터망 즉 호상 정보를 교환하기 위하여 두대이상의 콤퓨터가 가지고 있는 능력이라고 생각하게 된다. 사실 다른 형태의 망 즉 전화망, 라지오망, 텔레비존망도 있다. 지어 사람들이 서로 만나 교제하는 련락망도 구성할수 있다.

이 장에서 망의 의미는 첫번째의것 즉 일정한 형태의 통신체계를 통하여 정보를 교환하는 두개 혹은 그이상의 기구들의 모임인것이다.

망 장 치 들

망장치란 서로 다른 체계사이의 자료교환을 위하여 여러개의 망마디들을 서로 련결하는데 쓰이는 콤퓨터 혹은 위상구조에 따라 달라 지는 장치들을 말한다. 이러한 장치에는 반복기, 망다리, 경로기, 교환기가 속한다.

집선기

집선기는 한 계렬의 많은 콤퓨터들을 하나의 장소에 집중적으로 련결시키는데 쓰인다. 집선기는 꼬임쌍선으로 콤퓨터를 서로 련결한다. 매국이 하나의 망케블로 련결된 전통적인 이써네트망을 생각해 보라. 꼬임쌍선망은 이와는 다르다. 이것은 물리적으로 별형망이다. 매국에서 나오는 케블은 집선기를 통해서만 다른 국과 련결되여 있다.

집선기는 능동집선기와 피동집선기로 갈라 진다. 피동집선기는 자기의 모든 포구들중에서 들어 오는 신호를 분할하기만 한다. 능동집선기는 받은 신호를 다른 접근포구에 다시 송신해 준다. 능동집선기가 원격감시와 원격지원에 쓰인다면 피동집선기는 그렇지 못하다.

집선기(hub)란 단어는 망다리, 반복기, 경로기, 교환기나 이 모든것들을 종합적으로 부르는데 쓰이기도 한다.

반복기

반복기는 한 망마디에서의 신호를 원래의 신호세기로 다른 마디에 다시 보내준다. 반복기는 해당 매체와의 최대거리가 초과할 때 서로 거리가 매우 먼 망들에서 쓸수 있다. 실례로 10Base5망표준에서는 두개의 국사이에 최대 4대의 반복기를 사용한다. 하나의 동축케블토막이 1,500m이므로 반복기를 사용하면 망길이를 상당히 늘일수 있게 된다.

망다리

망다리는 물리적자료프레임에 있는 자료들을 읽고 그 전송자료가 자기의 반대켠에 있는 망에 보내여 지는 자료인가를 결정하는 방법으로 작업을 수행한다. 망다리는 통표고리형망과 이써네트망에 다 쓰인다. 망다리는 프레임의 목적지주소에 기초하여 복사해야 할 프레임을 복사만 하는 방법으로 두 곳을 통과하는 자료를 려과한다.

경로기

경로기는 망과 망사이에서 자료들을 경로조정해 주는데 쓰이는 보다 정교한 도구이다. 경로기는 망규약(실례로 IP)파케트에 있는 정보를 리용하여 그 파케트를 어데로 보내게 할것인가를 결정한다. 경로조정규약을 통하여 받은 정의된 설정값이나 정보에 기초하여 파케트를 어데로 보낼것인가에 대한 정보를 수집하고 보관하는 기능이 경로기에 있다. 많은 경로기들이 두개의 망을 련결시키는 능력밖에 없다면 더 큰 규모의 경로기들은 각이한 매체에 련결된 수백개의 련결망들에 쓰이기도 한다.

교환기

교환기라는 용어가 지금 점점 더 혼동되고 있지만 본질상 여러개의 포구들을 가진 망다리라고 볼수 있다. 교환기는 회전식교환기와 매우 근사하며 전통적으로 일정한 기간 여러 망들을 련결시키는데 리용되여 왔다. 두개의 망은 일정한 시간동안에 서로 련결된다. 그러나 오늘날의 교환기들은 이 기능만 있는것이 아니라 그 능력을 제고하는 경로선택지능도 가지고 있다.

망의 형태

망에는 크고작은 각이한 형태들이 있다. 수많은 콤퓨터애호가들은 자기 집 테두리안에서 자그마한 국부망(LAN:Local Area Network)을 운영하기도 한다. 소규모기업들도 자그마한 국부망을 운영한다. LAN이 정확히 어떤 경우에 LAN이 되지 않는가 하는 문제는 토론해 볼 문제이다. 그러나 보다 간단히 설명할수도 있다.

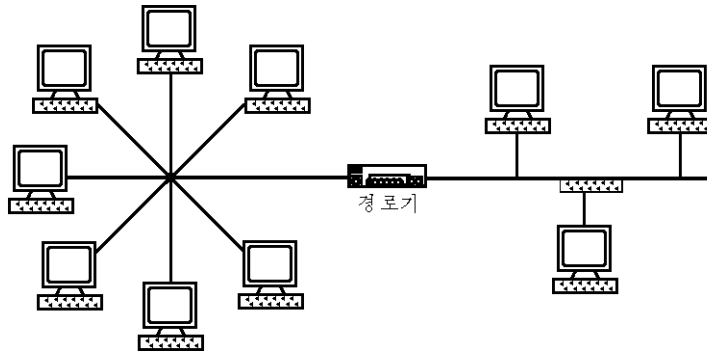



그림 5-1. 간단한 국부망

그림 5-1에서 볼수 있는것처럼 LAN은 한 건물의 같은 층에 있든 같은 방에 있든 상관없이 두개 혹은 그이상의 콤퓨터들을 서로 련결해 준다. 그러나 그 LAN이 그 국부지역밖의 다른 지역으로 확대되여 나가기 시작하면 그것은 벌써 LAN이 아니다. 실례로 어느 한 기관이 자기의 두 사무실을 도시의 서로 반대되는 끝에 두고 있으며 매 사무실에 각각 하나의 LAN을 운영한다고 하자. 이 두 LAN을 서로 련결하면 그림 5-2에서 보는것과 같은 도시망(MAN:Metropolitan Area Network)이 형성된것으로 된다.

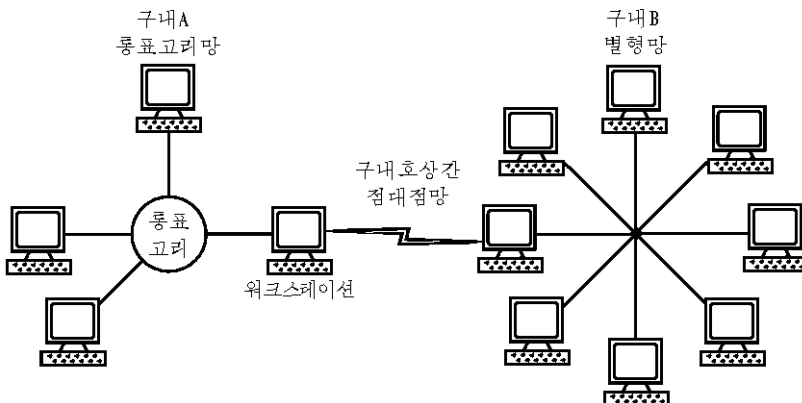



그림 5-2. 간단한 도시망

두개 혹은 그이상의 LAN이 동일한 지리적위치 즉 한 도시에 있는 경우에만 그것이 MAN으로 될수 있다는것을 잊으면 안된다. 례를 들어 그 기관이 뉴욕시에 두 사무실들을 가지고 있으면 그 련결망이 MAN으로 되지만 한 사무실이 뉴욕에 있고 다른 사무실이 쌘프랜씨스코에 있다면 더는 MAN이 될수 없고 이때에는 광지역망(WAN:Wide Area Network)이 된다.

이러한 망형태들이 결합되면 하나의 더 큰 망조직을 이루며 하나의 커다란 모임의 망들을 망라시켜 정보를 주고받게 된다. 사실상 그것이 인터네트 즉 국부망, 도시망, 광지역망들을 다 합쳐 묶어 놓은 인터네트로 되는것이다.

그러나 통신망은 개인이나 기관들로 하여금 위치에 관계없이 정보를 얻을수 있게 하지만 일련의 뚜렷한 부족점들도 있다. 이전에는 무엇을 훔치려면 건물을 뚫고 들어 가 책장이나 책상을 바로 찾고 물리적으로 그 무엇인가를 꺼내와야 하였다. 현재 정보가 직결상태에서 보관되고 있는 조건에서 사람들은 더 많은 정보를 잃고 있으며 또 그것을 잃을 가능성도 더 많다.

《도적》들이 물리적건물을 뚫고 들어 올 필요가 더는 없다. 망에서 《길》을 하나 찾아 도적질만 하면 되는것이다. 그러나 설계를 잘하고 보안대책을 잘 세워 놓으면 통신망은 결함보다 우점이 더 많을것이다.

그렇지만 망도 일정한 구조를 가져야 한다. 그러한 구조(혹은 위상구조라고도 한다.)는 하나씩하나씩 서로 련결된 콤퓨터처럼 간단한것도 있으며 많은 콤퓨터가 여러마디로 련결된 망처럼 복잡한것도 있다.

망의 위상구조

하나의 망에는 여러가지 마디가 있다. 매 마디에는 설계에 사용된 케블의 종류에 따르는 일정한 수의 콤퓨터가 있다. 이 망들은 각이한 방식으로 묶어 질수 있다.

점대점구조

점대점구조의 망은 그림 5－3에서 보는것처럼 정확히 두개의 망장치가 포함된 망이다. 이 형식에서 두 기구는 흔히 서로 모뎀이나 전화선으로 련결되게 된다. 다른 물리적매체 례하면 꼬임쌍선도 쓸수 있지만 전화선외에 그것들을 쓰는 경우는 상당히 특수한 경우이다. 이런 형식의 망에서는 공격이 이 두대의 콤퓨터자체 아니면 물리적준위의 련결선에서 진행되게 된다. 련결자체를 상사형모뎀으로 하기때문에 소리를 엿듣고 다른 콤

그림 5－3. 점대점구조

퓨터가 리해할수 있는 자료흐름을 구성하는것은 쉬운 일이다.

모선형구조

모선형망구조(그림 5－4)를 생각하면 10Base2 혹은 10Base5동축케블배선이 떠오르게 된다. 그것은 이러한 배선의 전기선구조가 모선 즉 전기선길이를 이루기때문이다. 이때 콤퓨터들은 케블형태에 따르는 접속기(connector)를 통하여 케블에 련결되게 된다.

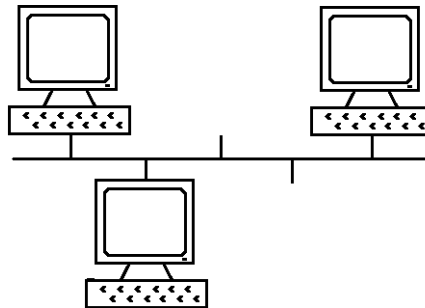



그림 5－4. 간단한 모선형구조

모선형망구조에서는 케블의 길이에 제한 받지 않는 한 누구도 몰래 콤퓨터엿보기도구나 망엿보기도구들을 부착시킬수 있다. 예비접속구 즉 쓰지 않는 접속구가 있으면 그 망을 통한 전송자료를 잡기 위한 망엿보기도구쯤 설치하는것은 어렵지 않다.

직렬련결형구조

직렬련결형망구조는 그림 5－5에서 보는바와 같이 피동의뢰기(thin-client: 의뢰기/봉사기체계에서 소유 총 비용의 삭감을 목표로 하는 의뢰기하드웨어의 구상안-역주)가 련결된 망이나 10Base 2동축케블로 련결된 망에 쓰인다. 이러한 환경에서의 국간련결은 다중전화선련결이나 점대점련결을 리용하여 콤퓨터들을 련결하는 점대점련결회선을 이루든가 아니면 국대국련결회선을 형성할수도 있다.

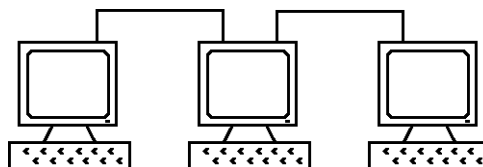



그림 5－5. 간단한 직렬련결형구조

그림을 보면 가운데국이 망기판을 두개 가지고 있는것으로 보이는데 그렇지 않다.

콤퓨터들이 같이 사슬형태로 묶어 진다는것을 보여 주기 위해서 그렇게 그려 놓은데 지나지 않는다. 피동의뢰기인 경우에는 케블 두개에 T형접속구를 써서 직접 워크스테이션에 그림 5—6처럼 련결시킨다. 이 그림은 콤퓨터들을 어떻게 직렬련결형으로 이어 주며 특히 10Base5 혹은 피동의뢰기망에서 어떻게 구성되는가를 보여 준다.

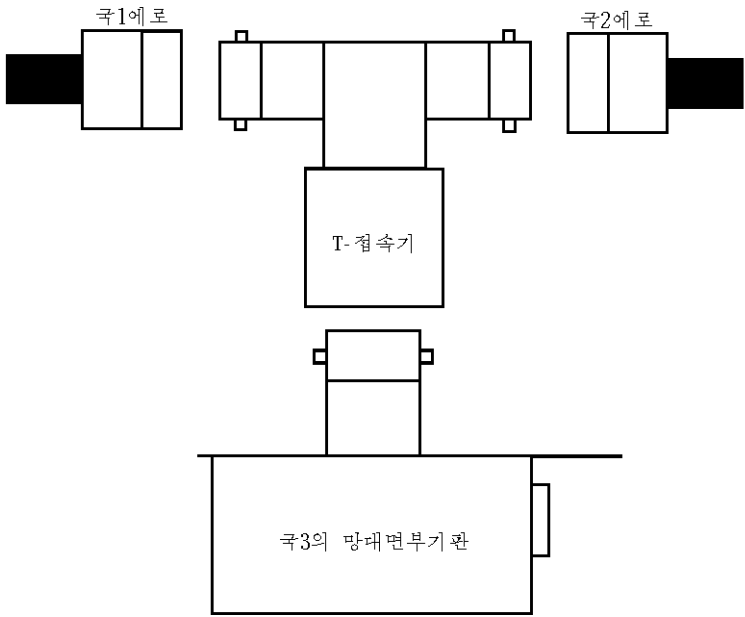



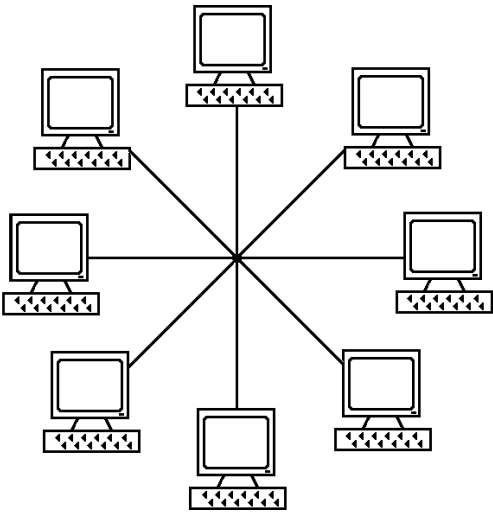
그림 5—6. 피동의뢰기결선

별형구조

그림 5—7. 간단한 별형구조

별형망(그림 5－7)은 흔히 꼬임쌍선형환경에서 많이 볼수 있는데 이런 망에서 매 콤퓨터는 별형망의 가운데에 있는 집선장치와 자기사이에 련결선을 가지는 형식으로 서로 련결되여 있다. 모든 콤퓨터들에서 나온 케블은 모두 가운데 있는 집선장치에서 끝나는데 이 집선장치가 매 케블을 전기적으로 련결시켜 그 망을 형성시켜 준다. 이 집선장치를 집선기라고 부른다.

이 망구조는 모선구조의 망과 꼭 같은 문제점들을 안고 있다. 합법적인 원래의 콤퓨터 한대를 다른것으로 교체하거나 별모양의 끝점 어디든지 아니면 가운데 있는 집선기에 엿보기도구(sniffer)를 붙이는것은 쉽다.

고리형구조

고리형망구조(그림 5－8)는 IBM통표고리망에서 가장 많이 볼수 있다. 이 망에서는 통표가 콤퓨터들사이로 전달된다. 통표가 없으면 그 어느 콤퓨터도 파케트를 방송할수 없다. 이런 식으로 통표를 리용하면 망에 있는 각국에서 통신을 주고받는 과정을 통제할 수 있다.

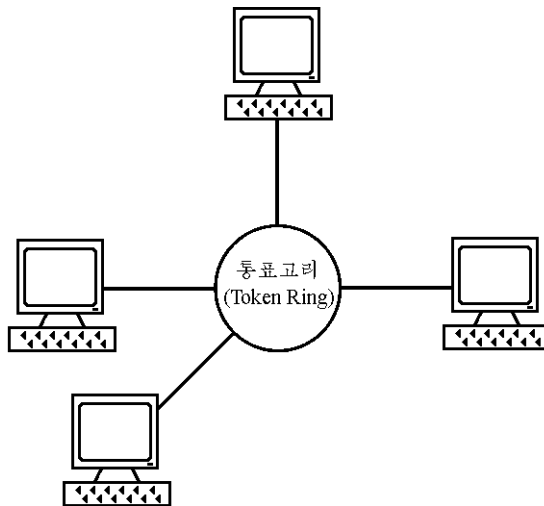



그림 5－8. 통표고리구조

그러나 통표고리형망구조는 보기에 고리형으로 보이지만 그림 5－8에서 보는바와 같이 전기배선상 별모양을 이룬다. 고리형망구조도 역시 매 콤퓨터가 다른 두개의 국과 통신을 어떻게 하겠는가를 알고 서로 련결되여 그림 5－9처럼 고리형태를 이룰 때에 형성되게 된다. 이것은 이 두개의 다른 콤퓨터들에 의거하여야 그밖의 다른 콤퓨터들과 통신을 할수 있다는것을 의미한다.

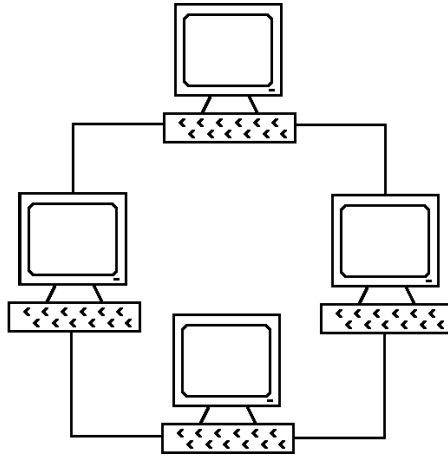



그림 5－9. 고리형구조

거미줄형구조(Web)

Web구조망(그림 5－10)은 복잡하며 규모가 크기때문에 유지하기가 힘들다. 이 망에서 매 콤퓨터는 다른 콤퓨터들과 련계를 자체로 짓게 된다. 사용중에 있는 콤퓨터가 많으면 많을수록 체계설정파일은 더 커지며 더 복잡하게 된다. 그러나 Web구조망은 앞에서 이미 본 형태의 망들에 비하여 여러가지 뚜렷한 장점들을 가지고 있다.

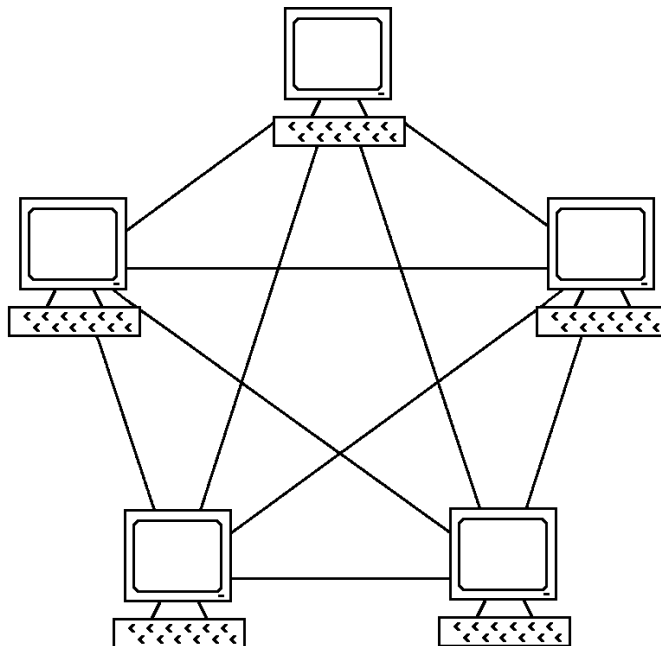



그림 5－10. Web구조

이 구조의 망은 다중고장이 있어도 그 콤퓨터가 다른 콤퓨터들과 통신을 할수 있게 하므로 상당히 강력한 구조의 망이다. 그림 5－10의 례를 리용해 보면 하나의 기계가 최고 4번까지의 실패를 체험할수도 있다. 4번의 실패나 고장이 있어도 콤퓨터는 Web과의 통신을 유지한다. 그 콤퓨터가 통신능력을 다 잃거나 망에서 제거되지 않는 한 자료의 흐름은 계속될것이다.

이것으로 하여 Web망은 망고장에 상당히 잘 견디며 망고장률이 높은 경우에도 자료흐름을 충분히 보장한다. 망회로구성가격과 유지운영비가 높음에도 불구하고 많은 기관들이 바로 이 특성으로 하여 이 망형태를 선택한다.

지금까지 설명한 매 망형태들은 자체의 고유한 망하드웨어와 위상구조를 가져야 정보통신을 할수 있다. 그 기술과 작용원리는 거의 모든 사람들에게 다 잘 알려 져 있다. 그리고 또 그렇게 모든 사람들에게 알려 져야 하는것이다.

망의 방식

망설비들은 일정한 형태의 물리적매체를 리용하여 련결되여야 한다. 케블로 련결하는 방법은 가장 많이 쓰이는 망련결방식이다. 그러나 오늘날의 망에는 무선망도 있는바 이것은 이동전화와 련결된 탁상형콤퓨터, 무릎형콤퓨터 혹은 손바닥콤퓨터에도 적용되고 있다. 여러가지 망결선방식이 있지만 가장 많이 쓰이는 방식은 이써네트와 통표고리형이다.

이 두가지 형태의 망구성, 그에 각각 해당되는 배선방식, 설비, 통신교환방법 등에 대하여 구체적으로 쓰자면 큰 책 몇권은 잠간 될것이다. 따라서 이 장에서는 그 력사와 각이한 매체형태들만 간단히 보려고 한다.

이써네트

이써네트는 의심할바없이 현재 가장 널리 쓰이고 있는 국부망기술이다. 원래의 가장 널리 쓰던 이써네트판은 10Mbps의 자료전송속도를 지원하였지만 새로 개발된 Fast Ethernet 와 Gigabit Ethernet라고 부르는 개정판들은 100Mbps와 1,000Mbps의 속도를 지원하고 있다.

이써네트LAN들의 구성은 동축케블, 특별한 등급의 꼬임쌍선 혹은 빛섬유케블로 배선한다. 망결선방법의 견지에서 볼 때 가장 인기 있는것은 모선형망배선방식과 별형망배선방식이다. 이써네트기구들은 《반송파수감다중접근/충돌검출》(CSMA/CD–Carrier Sense Multiple Access/Collision Detection)이라고 부르는 규약을 리용하면서 망접속을 서로 경쟁적으로 한다.

Xerox Palo Alto연구쎈터(PARC)의 봅 메트케이프와 데이비드 복즈는 1970년대에 시험적으로 첫 이써네트체계를 개발하였다. 이것을 리용하여 연구소에 Xerox Alto콤퓨터들과 레이자인쇄기를 련결하여 자료전송속도 2. 94Mbps(당시로는 소박하고 지금 수준에서는 낮은 속도임)를 보장하였다. Alto콤퓨터의 체계박자수때문에 당시 자료전송속도를 그

렇게 정하였다. 이써네트기술은 모두 10MbpsCSMA/CD규약에 기초한다.

10Base5방식 이것을 흔히 망결선기술의 할아버지라고 하는데 그것은 이 방식이 10mm동축케블로 10Mbps의 전송속도를 지원하는 원래의 이써네트체계이기때문이다. 10Base5라는 표기는 기저대역전송형태인 **10**Mbps의 전송속도와 **5**00m최고유효길이를 간략하여 쓴것이다. 실지 이 케블은 많은 경우 더는 쓰이지 않는다. 그러나 그 기능들과 사용에 대하여 간단한 언급을 할수 있다.

1980년 9월 Digital Equipment회사, 인텔회사, 제록스회사는 DIX표준이라는 이 세 회사의 첫 글자를 딴 첫 이써네트규격 1.0판을 내놓았다. 이 표준규격에는 《굵은》이써네트체계(10Base5)에 대한 정의도 들어 있는데 여기서 《굵은》이라는것은 망설비배선에 쓰이는 그 굵은 동축케블이라는 뜻이다.

워크스테이션위치를 명백히 하기 위하여 10Base5 굵은 이써네트동축케블에는 2.5m마다 표식을 해놓아 거기에 송수신기(다중접속장치 MAU : Multiple Access units)들을 붙일수 있게 되여 있다. 송수신기들을 2.5m마다 련결해 놓으면 전송질을 떨어 뜨리는 신호잡음을 최소화할수 있다.

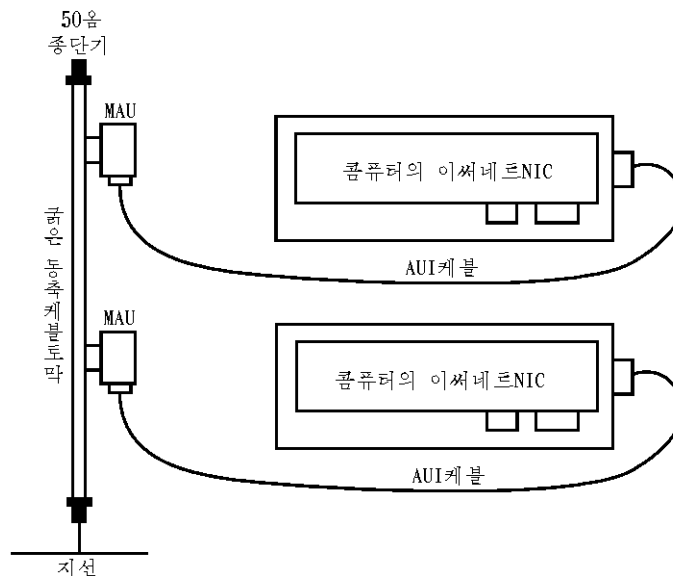



그림 5－11. 10Base5국결선방식

10Base5 송수신기는 케블에 구멍을 뚫어 전기케블과의 접촉을 보장하는 조임쇠에 꽉지를 련결하는 방법으로 붙인다(그림 5－11을 볼것). 송수신기들은 비침입성꽉지라고 부르는데 그것은 전송정보흐름을 방해하지 않고 살아 있는 망에 결선할수 있기때문이다.

국들을 송수신기에 련결하려면 부착단위대면부 즉 AUI라고 하는 송수신기케블을 통해야 한다. 표준적으로는 10Base5에 련결되는 콤퓨터국에는 이써네트망대면기판(NIC) 한개 혹은 15핀AUI포구를 가진 적응기기판이 하나 있다. 그렇기때문에 많은 망기판들은 오늘도 15핀AUI포구를 가지고 있다.

10Base5동축케블 한 경간의 길이는 최고 500m이며 2. 5m간격으로 최고 100대의 송수신기를 하나의 경간에 련결할수 있다. 10Base5케블경간이라는것은 끊기지 않는 련속적인 케블구간도 될수 있고 끝을 서로 이어 놓은 여러 케블토막의 결선일수도 있다.

10Base5배선으로 잘 설치하면 신뢰성이 매우 높을수 있으며 현존 케블경간내에서 따기방법으로 새로운 국들을 쉽게 추가할수 있다. 그러나 케블자체가 굵고 무거우며 유연성이 부족하므로 설치하는데 난관이 있다. 게다가 모선형위상구조에서는 문제가 제기된 국을 고립시키기가 어려우며 그 동축케블은 지금까지 나온 더 높은 망통신속도를 지원하지 못하는 점도 있다.

10Base2 방식 《가는》이써네트, 값 눅은 네트(cheapernet) 혹은 10Base2라고도 불리우는 제2판 이써네트는 1985년에 나왔다. 이 두번째판 이써네트는 보다 가늘고 보다 눅은 동축케블을 써서 망배선을 간단하게 해준다. 비록 이 두가지 즉 가는 체계와 굵은 체계가 망의 성능은 상당히 개선시켜 주지만 모선형위상구조를 리용하기때문에 망변경이 어려우며 신뢰성측면에서 미흡한 점이 많다. 이 10Base2방식은 굵은이써네트표준이후에 나와서 처음으로 도입된 물리적매체의 변종이였다.

굵은형이써네트와 가는형이써네트는 둘다 같은 망특성들을 가지고 있지만 10Base2에 쓰이는 가는케블은 10Base5에서 쓰이는 굵은케블보다 더 눅고 더 가벼우며 더 유연성 있고 설치하기 더 쉬운 장점들을 가지고 있다. 그러나 가는케블은 전송특성이 굵은것보다 좋지 못한 결점도 있다. 가는케블은 최고경간길이가 185m(10Base5가 500m인데 비하여)인데다가 매 케블경간당 최고 30대의 국(10Base5가 100대인데 비하여)을 허용한다.

10Base2에서는 10Base5에서처럼 선따기방법으로 련결하는것이 아니라 BNC T형접속기를 통하여 송수신기를 련결한다. 그 이름이 보여 주는것처럼 BNC T형접속기는 T자처럼 생겼다. 케블을 따라 흐르는 자료전송에 영향을 주지 않고 새로운 국을 추가할수 있는 10Base5와는 달리 10Base2(그림 5－12에서처럼)에서는 망을 끈 다음에야 새로운 국을 설치할수 있다. 이런 방법으로 국들을 추가설치하거나 해체하는것은 여기에 쓰이는 접속구때문이다. 즉 이렇게 새국을 련결시키려면 케블을 자르고 거기에 BNC T형접속구를 끼워 넣어야 하기때문이다. 주의하여 련결하지 못하는 경우 제대로 련결되지 않은 접속구때문에 망전송자료들의 흐름이 장애될수 있는 가능성이 있다.

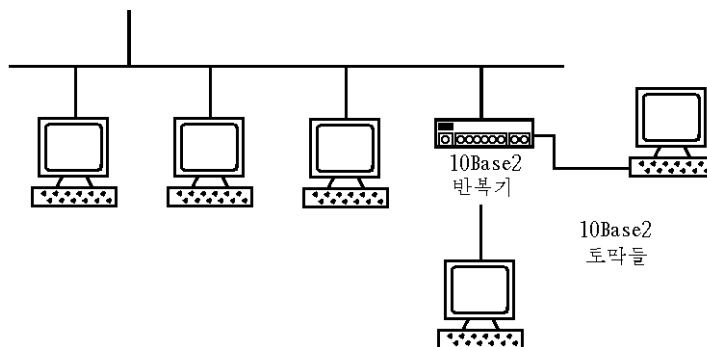



그림 5－12. 10Base2망

BNC T형접속구는 콤퓨터의 이써네트망대면기판(NIC)에 직접 꽂을수도 있고 아니면 외부에 있는 가는이써네트의 송수신기에 꽂고 그것을 표준AUI케블을 거쳐 NIC에 꽂을수도 있다. 만일 망에서 국들을 해체하는 경우에 BNC T형접속구는 떼고 그대신 BNC관형접속구를 끼워 선로가 직선으로 련결되게 한다.

10Base2배선에 쓰이는 가는동축케블은 10Base5에서 쓰이는 굵은케블에 비하여 설치작업하기가 상당히 쉬우며 외부적인 송수신기를 없앰으로써 망설치비용이 더 눅다. 그러나 표준설치에서는 그림 5－5에서 본바와 같이 직렬련결이므로 신뢰도가 낮고 고장퇴치가 더욱 어렵다. 게다가 일부 사무실환경에서는 직렬련결구간설치가 어려우며 10Base5처럼 피동의뢰기망은 더 높은 망전송속도를 지원하지 못한다.

10Base–T방식 10Base2나 10Base5방식의 망에서처럼 10Base–T방식도 10Mbps의 전송속도만 지원한다. 그러나 이러한 기술들과는 달리 10Base–T방식은 음성급이나 3부류급 혹은 더 좋은 전화회선망에 바탕을 두고 있다. 이 배선을 흔히 꼬임쌍선이라고 하는데 여기서 한 쌍선은 자료전송에 그리고 다른 쌍선은 자료수신에 쓰인다. 이 배선의 량쪽 끝에는 RJ–45 8자리꽂개가 있어야 한다. 꼬임쌍선이 급속히 사용됨으로써 10Base–T방식이 오늘 가장 인기 있는 이써네트판으로 되였다.

모든 10Base–T결선은 점대점결선이다. 이것은 10Base–T케블이 량끝에 최고 두대의 이써네트송수신기(즉 다중접속장치인 MAU)들을 가질수 있다는것을 의미한다. 한쪽 끝은 표준적으로 10Base–T집선기에 련결된다. 다른 끝은 직접 콤퓨터국의 망대면기판(NIC)이나 외부적인 10Base–T송수신기에 꽂으면 된다. 오늘날의 NIC에는 송수신장치 즉 다중접속장치가 집적되여 있다. 즉 외부적인 송수신장치가 필요없이 케블을 직접 꽂는다는것을 의미한다. 만일 AUI포구가 있는 이전카드는 있는데 RJ–45꽂개가 없다면 할수없이 눅은 외부다중접속장치를 써서 련결해야 할것이다.

10Base–T배선방식이 별형망구성에서만 사용되여야 한다는 요구는 없다. 이 방법은 두 망기구들을 점대점으로 련결시키는데 많이 쓰인다. 이런 형의 배선을 형성할 때에는 교차케블을 써서 수신쌍선과 송신쌍선을 갈이 련결하여 자료의 흐름을 보장해야 한다. 기타 모든 경우에는 직선 혹은 보통케블을 쓴다. 비차페꼬임쌍선3부류의 10Base–T의 최고마디길이는 100m이다. 신호의 질적지표가 만족되는 한 더 긴 마디들도 쓸수 있다. 비차페꼬임쌍선 5부류와 같은 보다 질이 높은 케블은 표준적으로 요구되는 신호의 질을 유지하는 방향에서 마디길이가 150m쯤 더 길수 있다.

10Base–T를 점대점케블련결하면 그림 5－13에서 보는바와 같이 별모양의 위상구조가 생긴다. 별형위상구조에서 별모양의 가운데에는 집선기가 있어 점대점련결이 마치도 별빛이 가운데서 밖으로 퍼져 나가는듯이 보인다. 별형위상구조는 보수가 간단하며 고장퇴치도 보다 빠르며 케블고장이 나도 어느 한 고리에만 영향을 주게끔 고립시킬수 있다.

10Base–T선이 송신선과 수신선을 따로 가지고 있는것으로 하여 쌍방향조작기능을 선택적으로 지원할수 있게 한다. 쌍방향기능을 지원하기 위해서는 NIC와 집선기에 쌍방향조작기능이 있어야 하며 또 그렇게 설정되여 있어야 한다.

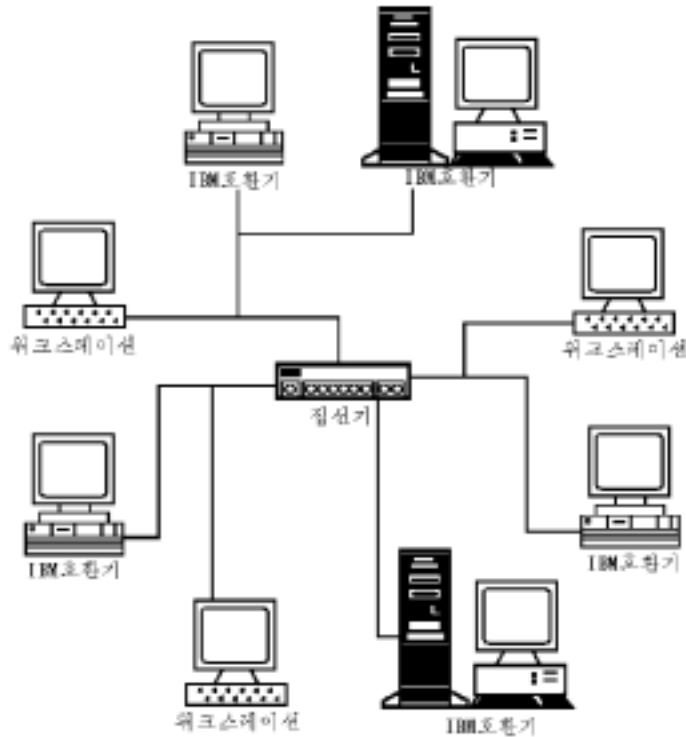



그림 5－13. 10Base–T별형구조

10Broad36방식 10Broad36은 LAN환경에서는 널리 쓰이지 않는다. 그러나 MAN이나 WAN환경에서는 쓰일수 있으므로 간단히 설명한다. 10Broad36은 광대역케블체계에서 10Mbps의 전송속도를 지원한다. 여기서 《36》은 두 국간의 최대 마디길이가 3,600m이라는것을 의미하며 이런 형의 망은 케블TV(CATV)전송체계에서 쓰이는것과 꼭 같은 누은 동축케블을 쓴다.

기초대역망기술에서는 하나의 전기적신호를 전송하는데 전체 대역을 다 리용한다. 이때 이 신호는 아무러한 변조가 없이 송신기에 의하여 매체에 전달된다. 이 기술은 기초대역망기술의 생산과 유지에 드는 비용을 낮추며 10Broad36을 제외한 이써네트체계에서 다 쓰인다.

광대역에서는 충분한 대역을 리용하여 다중신호를 매체에 내보낸다. 이때의 신호들로는 육성, 화상, 자료정보들이 될수 있다. 전송매체는 여러개의 통로로 나뉘여 지며 매 통로는 보호통로를 사이에 두고 서로 나누어 진다. 보호통로는 간섭을 방지하기 위하여 통로들사이에 있는 빈주파수공간이다.

광대역케블은 10Base5와 10Base2에서 리용하던 기초대역동축케블보다 더 먼거리의 전송을 할수 있는 우점을 가지고 있다. 한 토막의 10Broad36은 1,800m정도까지 갈수 있다. 10Broad36에서는 광대역케블에 물리적으로 또는 전기적으로 련결시킬수 있는 송수신기를 쓰면 국들을 더 추가할수 있다. 콤퓨터와 송수신기의 련결은 10Base5의 배선에서와 같이 AUI케블을 통하여 수행한다.

10Broad36이 도입되였을 때 이 방식은 10Base5나 10Base2보다 훨씬 더 긴 마디를 지원하는 우점을 가지고 있었다. 그러나 빛섬유케블이 도입되면서 이 우점은 점차 사라지게 되였다. 10Base2나 10Base5와 마찬가지로 10Broad36은 더 높은 망속도가 불가능하며 완전2중운영방식도 지원하지 못한다.

반복기들사이의 빛섬유결선

반복기들사이의 빛섬유결선(FOIRL)은 두개의 빛섬유케블상에서 10Mbps의 점대점련결을 보장하기 위하여 개발되였다. 표준규격에서 규정한바와 같이 FOIRL은 두개의 반복기사이의 련결에만 한정되여 있다. 그러나 업체들에서는 그 기술을 개조하여 한 콤퓨터와 한 반복기사이의 장거리련결도 지원하게 하였다.

10Base–FL 지금까지 설명한 이써네트망에서처럼 10Base–FL(FL은 fiber link를 의미)은 10Mbps의 전송속도를 지원한다. 두개의 빛섬유케블을 리용하여 2중능력인 송신수신능력을 제공한다. 모든 10Base–FL마디들은 점대점으로 송수신기로 련결된다. 이것은 두개의 경로기나 망장치들을 서로 련결시키는데 가장 많이 리용될수 있다는것을 의미한다. 콤퓨터한대를 련결하자면 외부적인 10Base–FL송수신기를 리용해야 한다.

10Base—FL은 건물들사이의 망결선보장에 널리 쓰인다. 보다 긴 마디의 길이를 지원할수 있으며 번개나 지면전류 같은 전기적피해에 견딜수 있는 능력을 가지고 있음으로 하여 망이 입을수 있는 피해를 미리 막는데 리상적이다. 빛섬유는 또한 발전기나 기타 전기설비가 내는 전기적잡음에는 면역이 크다.

10Base—FB 10Base–FL처럼 대체로 콤퓨터를 련결하는데 쓰이는것이 아니라 10Base–FB(FB는 fiber backbone을 의미)는 10Mbps의 전송속도로 최량화된 특수동기신호결선으로 반복기를 서로 련결해 준다.

10Base–FL이 콤퓨터와 반복기를 련결하는데 쓰인다면 10Base—FB는 반복기사이의 점대점결선에 쓰인다. 10Base–FB선 량쪽에 있는 반복기가 이 결선을 지원하게 되여 있는것은 다름아닌 자기의 독특한 신호발생적특성과 그 사용수법이 있기때문이다. 따라서 10Base–FB를 10Base–FL용반복기끝에 련결할수 없다. 그것은 10Base–FL반복기가 10Base–FL신호발생을 지원하지 않기때문이다.

10Base–FP 10Base–FP(FP는 fiber passive를 의미)망은 빛섬유피동별형체계상에서 10Mbps의 전송속도를 지원한다. 그러나 완전2중전송은 지원하지 못한다. 10Base–FP별형은 피동적인 장치로서 직접적인 전원은 필요로 하지 않으므로 직접적인 전원공급이 없는 곳에서 쓰인다. 이 별모양장치자체는 최고 33개의 워크스테이션을 련결시킬수 있다. 이 별형위상구조는 피동집선기로서 특수한 10Base–FP송수신기로부터 빛신호를 받는다(그리고 전송자를 포함한 별형위상구조에 련결된 모든 기타 10Base–FP송수신기에 그 신호를 피동적으로 골고루 분배한다.).

100Base–T 100Base–T라는 식별표시는 그 어떤 망형식을 가지는것이 아니라 여러가지 망형태 즉 100Base–TX, 100Base–FX, 100Base–T4, 100Base–T2에 대한 통칭이다. 이것들을 다 고속이써네트(Fast Ethernet)라고 한다.

100Base–T체계들은 흔히 자동인식이라고 하는 공정을 리용하여 10 혹은 100Mbps의

전송속도를 지원한다. 이 공정을 쓰면 련결되여 있는 장치로 하여금 얼마만한 속도로 가동하겠는가를 결정하게 한다. 10Base–T망련결은 내장형매체독립대면부(MII)를 가진 NIC를 통하여 하든가 혹은 앞에서 언급된 망에서 쓰는 MAU와 매우 류사한 외장형MII를 통하여 한다.

100Base–TX 100Base–TX는 두쌍의 꼬임쌍선케블상에서 100Mbps의 전송속도를 지원한다. 두쌍중의 한쌍은 자료송신에 쓰이며 다른 한쌍은 자료수신에 쓰인다. 두쌍의 꼬임쌍선들은 하나의 케블에 넣었는데 여기에는 흔히 두쌍의 보충선들이 있다. 만일 두쌍의 보충 및 예비쌍선들이 있으면 쓰지 말고 그냥 두어야 한다. 그것은 그 케블로 다른 신호들과 같이 쓸 때 생기는 간섭(crosstalk)을 허용하게끔 10Base–TX가 설계되지 않았기때문이다. 케블의 량쪽끝에는 8위치 RJ–45접속구가 하나씩 달려 있다.

100Base–TX는 100Ω짜리 제5부류비차폐꼬임쌍선(UTP)케블에서 최고 100m전송을 지원한다. 제5부류케블은 10Base–T에서 쓰이는 제3부류케블보다 더 높은 급의 배선이다. 이것은 최고 100MHz의 주파수에서의 전송이다. 여러가지 부류의 꼬임쌍선케블에 대해서는 표 5－1에서 언급된다.

표 5－1　　　　꼬임쌍선부류와 정격

다음의것들이 UTP(비차폐꼬임쌍선)케블부류이다.	
제1부류와 제2부류	이써네트에 사용하기 적합치 않음.
제3부류	최고 16MHz까지의 주파수전송을 지원하는 전기적특성과 100Ω의 완전저항을 가진 비차폐꼬임쌍선. TIA/EIA 568–A 규격명세서에서 규정됨. 100Base–T, 100Base–T4, 100Base–T에서 사용할수 있음.
제4부류	최고 20MHz까지의 주파수에서 전송지원하는 전기적특성과 완전저항 100Ω인 비차폐꼬임쌍선. TIA/EIA 568–A 규격명세서에 규정됨. 10Base–T, 100Base–T4, 100Base–T2에서 사용할수 있음.
제5부류	최고 100MHz까지의 주파수에서 전송지원하는 전기적특성과 완전저항 100Ω인 비차폐꼬임쌍선. TIA/EIA 568–A 규격명세서에서 규정됨. 10Base–T, 100Base–T4, 100Base–T2, 100Base–TX에서 사용할수 있음. 100Base–T는 지원할수 있으나 케블이 100Base–T 규격명세를 만족시키는가를 확인하기 위하여 검사해야 함.
제5e부류	제5e부류(혹은 Enhanced Cat5 즉 성능갱신판 5부류)는 새 규격으로서 제5부류를 증가하는 전송능력이다. 제5부류와 마찬가지로 이 부류는 완전저항 100Ω에 100MHz까지의 주파수에서의 전송을 지원하는 전기적특성을 가진 비차폐꼬임쌍선이다. 그러나 NEXT(근단말새기), PSELFEXT(전력합등준위원단말새기)와 감쇠현상을 갱신한 규격명세서를 가지고 있다. TIA/EIA 568–A표준갱신항목에서 규정예견됨. 1000Base–T에서 리용할것을 목적하고 있으나 10Base–T, 100Base–T4, 100Base–T2, 100Base––TX도 지원함.
제6부류	최고 250MHz까지의 주파수와 100Ω의 완전저항을 가진 꼬임쌍선에서의 전송지원을 예견한 표준안
제7부류	최고 600MHz까지의 주파수와 100Ω의 완전저항을 가진 꼬임쌍선에서의 전송지원을 예견한 표준안

모든 100Base–TX마디들은 점대점으로 매끌에 하나의 송수신장치가 붙어 있다. 대부분의 100Base–TX결선은 콤퓨터국을 집선기에 잇는 방법으로 한다. 100Base–TX집선기는 표준적으로 송수신장치를 내부적으로 가지고 있다. 그러므로 제5부류케블꽂개를 직접 집선기에 잇는 RJ–45접속구에 꽂으면 된다. 콤퓨터국의 련결은 NIC를 통하여 실현된다. 송수신장치의 기능이 NIC에 집적되여 있으므로 제5부류꼬임쌍선케블을 직접 NIC에 있는 RJ––45에 꽂을수 있다. 그렇지 않으면 MII를 리용하여 케블을 콤퓨터에 련결할수도 있다.

100Base–FX 100Base––FX는 두줄의 빛섬유케블로 100Mbps의 전송속도를 보장하며 한방향 혹은 쌍방향전송을 둘다 지원한다. 기본적으로는 100Base––TX의 빛섬유판이라고 볼수 있다. 모든 꼬임쌍선들은 빛섬유들로 교체되고 있다.

100Base–T4 100Base–T4는 4쌍의 제3부류 혹은 보다 더 좋은 꼬임케블망에서 100Mbps의 전송속도를 보장한다. 100Base–TX가 요구하는 제5부류와는 반대로 보다 눅은 제3부류케블을 쓰는 100Mbps이써네트를 지원한다.

100Base–T4에 쓰이는 4쌍의 선들중에서 한쌍은 자료전송, 다른 쌍은 자료수신에 쓰이며 남은 두개의 쌍방향케블은 송신 혹은 수신에 쓰인다. 이러한 배렬로 하여 3쌍의 선들이 자료전송에 리용되며 한쌍은 전문적으로 망접속에서의 충돌을 방지하는데 항상 리용되게 된다.

100Base–T4는 100Mbps로 자료전송 및 수신을 동시에 하지 못하므로 완전쌍방향운영방식을 지원하지 못한다.

1000Base–X 1000Base–X라는 표식은 기가비트망을 이루는 표준을 의미하는것이다. 기가비트망에는 1000Base–LX, 1000Base–SX, 1000Base–CX, 1000Base–T가 있다. 이 기술들은 다같이 기가비트이써네트장치의 매체접근조종(MAC) 및 물리층기능들을 가진 기가비트매체독립대면부(GMII)를 리용한다. GMII는 10Mbps이써네트의 부착장치대면부(AUI) 그리고 100Mbps이써네트의 매체독립대면부(MII)와 상사적이다. 그러나 AUI나 MII와는 달리 GMII에서는 그 어떤 접속구도 쓰지 않고 송수신장치와 외부적인 케블을 통하여 련결된다. 모든 기능들은 직접 기가비트이써네트장치에 있으며 앞에서 언급한 GMII는 다만 내적부분품에 지나지 않는다.

1000Base–LX 이 케블은 장파레이자를 리용하여 빛섬유케블로 자료를 전송한다. 단일방식과 다중방식빛섬유(후에 설명함)가 다 지원된다. 장파레이자는 단파레이자보다 더 비싸지만 보다 긴 거리에 도달하는 장점을 가지고 있다.

1000Base–SX 이 케블은 단파레이자를 리용하여 빛섬유케블로 자료를 전송한다. 다중방식빛섬유만 지원된다. 단파레이자는 장파레이자보다 눅은 장점을 가지고 있다.

1000Base–CX 이 배선방식은 twinax 혹은 short haul copper라고도 부르는 특별한 차페균형동좌퍼케블을 사용한다. 마디길이는 25m로 제한되는데 이렇게 되면 1000Base–CX가 배선실 같은 좁은 공간에서 설비를 련결시키는데만 쓰이게 된다.

1000Base–T 이 배선방식은 제5부류균형동축케블 100m의 기가비트이써네트를 지원한다. 4쌍의 제5부류배선상에서 완전2중전송방식이 가능하다. 총체적인 자료전송속도 1000Mbps를 보장하려면 매 쌍선으로 250Mbps의 자료전송속도가 보장되여야 한다.

통표고리

통표고리형은 이써네트다음으로 가장 많이 쓰이는 국부망(LAN)기술이다. 통표고리형 국부망의 국들은 고리형의 위상구조를 이루며 여기서 자료들은 고리형국 하나에서 다음 국으로 순차적으로 전송되는 방식을 취한다. 통표를 순환시키는 방식으로 고리전체를 초기화한다. 고리상에서 자료전송하기 위해서는 하나의 국이 통표를 잡아야 한다. 정보를 전송하면 정보를 국에 전달하는 프레임이 그 통표를 밀어 낸다. 그 프레임은 고리를 순환하면서 하나 혹은 그이상의 목표국들에서 복사된다. 그 프레임이 송신국에 되돌아 오면 그것은 고리망에서 제거되며 새로운 다른 통표가 전송된다.

1980년대 초 IBM회사는 스위스의 쮸리히에 있는 자기의 연구소에서 이 통표고리형망을 처음으로 규정하였다. IBM은 통표고리형망의 표준화를 추진하였으며 그 이후 1985년에 원래 IBM개인콤퓨터의 갱신본인 첫 통표고리망제품을 도입하였다. 초기통표고리제품들은 4Mbps로 가동하였다. IBM회사가 아닌 다른 회사들도 각기 자체의 통표고리망관련설비를 개발할수 있는 소편을 제작할수 있도록 하기 위하여 IBM은 Texas Instruments와 공동개발에 들어 갔다. 1989년에 IBM은 통표고리형망의 전송속도를 4배로 높여 통표고리형제품도입에서 처음으로 16Mbps를 보장하였다.

1997년에 전용통표고리(DTR)망이 도입되였는데 이것은 전용 즉 완전쌍방향운영체계였다. 전용통표고리망은 보통의 통표넘기기규약을 생략하여 두 국간의 점대점련결상에서 통신을 보장할수 있게 한다. 이렇게 되면 매국이 전송과 수신을 동시에 하게 되여 있기때문에 전송속도가 배로 높아 지게 된다. 이렇게 되면 총체적으로 자료전송속도 32Mbps를 얻는것으로 된다. 1998년에 새로운 100Mbps의 통표고리제품이 하나 개발되여 이 갱신속도로 전용운영이 가능하게 되였다.

고리 통표고리망에서 고리는 전송매체인 케블과 그에 련결된 고리국을 포함한다. 많은 사람들이 통표고리를 고리망의 위상구조로 생각하는데 그렇지 않다. 통표고리망은 그림 5－8에서 보는것처럼 별모양으로 배선된 고리형위상구조이다.

매국은 통표고리적응기기판을 가지고 있어야 하며 돌출케블을 리용하여 집선기에 결선될수 있다. 집선기와 집선기들사이의 결선은 련결부(patch) 혹은 중계선케블을 통하여 집선기에 있는 고리입구 혹은 고리출구포구들에 꽂는 방법으로 한다. 집선기자체는 흔히 다국간접근장치(MSAU)라고 한다.

고리의 매국은 고리의 웃부분의 가장 가까운 국에서 자료를 받아 아래부분의 가장 가까운 국에 그것을 넘겨 준다. 즉 그것은 통표고리망에서 자료가 순차적으로 매국으로 중계된다는것을 의미한다. 자료를 받을 국은 자료가 지나갈 때 그 자료를 인차 복사해 놓는다. 전송자료가 원래의 송신자국에 다시 돌아 오면 고리에서 제거된다. 국은 통표가 지나갈 때를 포착하면 망상의 자료전송권(프레임이라고도 함)을 획득한다. 통표자체도 고유한 신호렬을 가진 프레임으로서 프레임전송후에 매번 망에서 순환된다.

정확한 통표를 포착하자마자 매국은 자체로 통표에 포함된 자료를 수정한다. 통표자료에는 다음과 같은것들이 포함된다.

- 조종마당 및 상태마당

- 주소마당
- 경로조정정보마당
- 정보마당
- 검사합

자료전송을 끝낸후 국은 새로운 통표를 전송하여 다른 국들이 고리접근권을 가지고 자기자료들을 전송할수 있게 한다.

일부 이써네트형망들에서처럼 통표고리망들은 삽입 및 우회방식이 있어 국들이 망에 들어 갈수도 있고 떠날수도 있게 한다. 국이 우회방식에 놓이면 돌출케블이 《감싸여》 국에 들어 가 있게 되므로 국자체가 하나마디망상에서 자체검사와 진단검사를 할수 있게 된다. 이 방식에서는 련결되여 있는 고리에서 참가권을 잃게 된다. 집선기가 《유령드라이브》신호를 받아야 국이 고리에 삽입된다.

통표고리는 4Mbps 혹은 16Mbps의 속도로 운영되며 고전통표고리라고 알려 져 있다. 전용통표고리라는 고속운영체계도 있다. 오늘날의 통표고리적응기(adapter)는 망에 꽂을 때 현재의 망속도를 탐지하고 그 속도에 맞추는 기능의 회로를 포함한다.

케블의 종류

이 부분에서는 보다 널리 쓰이는 케블형태들과 그 사용법의 일부를 보기로 한다(표 5－2).

꼬임쌍선

꼬임쌍선케블이 이렇게 명명된것은 선쌍이 서로 감겨 꼬였기때문이다. 매 선쌍은 서로 꼬인 두개의 절연된 통선으로 이루어 져 있다. 선쌍을 함께 꼬아 놓음으로써 회로에서의 간섭을 줄이고 장애를 감소시킬수 있게 한다.

비차폐꼬임쌍선케블(UTP) 비차폐꼬임쌍선케블은 오늘날 많이 리용되고 있다. UTP라고도 알려 진 이 케블은 차페가 없고 모든 꼬임쌍선형태는 《부류》준위에 기초하여 등급이 매겨 져 있다. 이 부류준위는 케블이 받아 들일수 있는 한계가 얼마이며 그것을 리용하여 실현하는것이 무엇인가를 결정한다.

UTP는 여러쌍의 100Ω케블이지만 일반적으로는 보통피복으로 피복된 4쌍의 선을 포함하고 있다. 10Base–T, 100Base–TX 그리고 100Base–T2는 꼬임쌍선 두개만을 리용하며 한편 100Base–T4와 1000Base–T는 모두 4개의 꼬임쌍선을 요구한다.

칸막이차페꼬임쌍선케블(ScTP) 칸막이차페꼬임쌍선은 네선쌍모두를 단일한 금속박막이나 꼬임선으로 차페된 4쌍의 100Ω UTP(비차페꼬임쌍선)이다. 이 박막이나 선으로 꼰 차페막은 EMI복사를 최소로 만들며 외부잡음에 대한 감수성을 최소화한다. 이러한 형태의 케블은 박막꼬임쌍선 혹은 칸막이차페 UTP(CsUTP)라고도 알려 져 있다. 기술적으로

칸막이차페된 꼬임쌍선은 금속박막으로 차폐된 비차페꼬임쌍선과 같다. 이것은 UTP도선등가부류와 같은 방법으로 이써네트응용에서 사용되고 있다.

차페꼬임쌍선케블(STP) 이 형태의 케블은 기술적으로 차페꼬임쌍선형이며 통표고리형망에서 리용되는 배선을 서술하는데 가장 일반적으로 사용되는 용어이다. 매 꼬임쌍선은 개별적으로 차페된 금속박막이 감겨 져 있고 전면에 걸쳐 꼰 끈으로 테를 두른 차페선으로 에워 싸여 있다. 이 준위의 차페는 EMI복사와 말새기(cross-talk)를 최소화한다. 이 케블은 일반적으로 이써네트와 함께 사용되지는 않으며 한편 이것은 완전저항정합변압기의 리용과 같은 용도에 적응시킬수 있다.

표 5-2 케블의 형태와 속성

표준속도	토막당 자료마디	위상 구조	매체	최대케블토막의 길이(m)	단방향	쌍방향
10Base5	10Mbps	100	모선형	단일50Ω동축케블(굵은이써네트)(10mm굵기)	500	미확인
10Base2	10Mbps	30	모선형	단일50ΩRG58동축케블(가는 이써네트)(굵기5mm)	185	미확인
10Broad36	10Mbps	2	모선형	단일75Ω CATV광대역케블	1,800	미확인
FOIRL	10Mbps	2	별형	두개의 빛섬유케블	1,000	1,000이상
1Base5	1Mbps		별형	두쌍의 꼬임전화케블	250	미확인
10Base–T	10Mbps	2	별형	두쌍의 100Ω 3부류 혹은 그 보다 높은 UTP케블	100	100
10Base–FL	10Mbps	2	별형	두개의 빛섬유케블	2,000	2,000 이상
10Base–FB	10Mbps	2	별형	두개의 빛섬유케블	2,000	미확인
10Base–FP	10Mbps	2	별형	두개의 빛섬유케블	1,000	미확인
100Base–TX	100Mbps	2	별형	두쌍의 100Ω 5부류 UTP케블	100	100
100Base–FX	100Mbps	2	별형	두개의 빛섬유케블	412	2,000
100Base–T4	100Mbps	2	별형	네쌍의 100Ω 3부류 혹은 그 이상의 UTP케블	100	미확인
100Base–T2	100Mbps	2	별형	두쌍의 100Ω 3부류 혹은 그 이상의 UTP케블	100	100
1000Base–LX	1Gbps	2	별형	장파레이자		
1000Base–SX	1Gbps	2	별형	단파레이자		
1000Base–CX	1Gbps		별형	특수차페평형동잡퍼케블묶음(쌍동축케블 혹은 short haul copper케블)	25	25
1000Base–T	1Gbps	2	별형	네쌍의 100Ω 5부류 혹은 그 이상의 케블	100	100

빛섬유

자료가 전기신호를 리용하여 전송되는 배선체계와는 달리 빛섬유는 빛을 리용한다. 이 체계는 전기신호를 빛으로 변환하고 그것이 가는 유리섬유를 통하여 전송되고 그것을 수신하는 국에서 다시 전기신호로 변환한다. 이것은 FOIRL, 10Base–FL, 10Base–FB, 10Base–FP, 100Base–FX, 1000Base–LX 및 1000Base–SX 통신표준용전송매체로서 리용된다.

빛섬유도선은 3개의 동심층으로 제조된다. 제일 중심층(혹은 속심)은 빛이 실제적으로 섬유를 통하여 전송되는 부분이다.

《피복》층은 두번째 층 즉 중간층을 이룬다. 이 층은 그것을 통하여 빛이 전달되지 못한다는것을 의미하는 더 작은 굴절지표를 가진다. 이것은 속심에 국한하며 빛신호가 유지되게 하는데 복무한다. 바깥층은 내부의 두 층에 대한 《완충》과 보호를 도모하는데 복무한다.

두가지 기본적인 형태의 빛섬유가 있다. 그것은 다자태빛섬유와 단일자태빛섬유이다.

다자태빛섬유(MMF) 두가지 형태의 MMF가 있다. 즉 개량형과 계단형이 있다. 개량형의 빛섬유는 속심의 바깥쪽으로 나가면서 작은 반사률을 가지며 속심의 중심으로 향하면서 점차적으로 증가된다. 이 지표는 빛섬유에서 신호분산을 감소시킨다. 계단형빛섬유는 속심에서 균일한 반사률을 가지며 속심/피복련결부에서 반사결수의 급격한 감소를 일으킨다. 계단형다자태빛섬유는 일반적으로 개량형다자태빛섬유보다 작은 대역너비를 가진다.

꼬임쌍선케블에 비한 다자태빛섬유의 근본장점은 그것이 보다 긴 토막길이를 가진다는것이다. 보안의 견지에서 꼬임쌍선케블우에서보다 빛섬유쌍에서 반송되는 정보에 접근하기가 훨씬 더 어렵다.

단일자태빛섬유(SMF) 단일자태빛섬유(SMF)는 단일한 빛의 자태만을 지원하는 작은 속심직경을 가진다. 이것은 대역너비를 제한하는데서 주요인자인 분산을 제거한다. 그렇지만 단일자태빛섬유의 속심직경이 작은것이 빛을 빛섬유에 결합시키는것을 더 어렵게 하며 그래서 비용이 많이 드는 레이자를 광원으로 리용하는것이 필요하다. 레이자광원은 LED들이 넓은 범위의 주파수를 내보내기때문에 SMF에서 높은 대역너비를 얻는데 리용되며 그래서 분산은 의미심장한 문제로 된다. 이것은 SMF망에서 실현과 유지보수를 위하여 비용이 더 들게 하고 있다. SMF는 MMF보다 훨씬 더 긴 토막길이를 지원할 수 있다. 토막길이 5,000m와 그이상이 자료전송속도 1Gbps까지에 걸쳐 모든 이써네트에서 지원된다는것이다. 그렇지만 SMF는 MMF보다 전개하는데 비용이 더 많이 든다는 약점이 있다.

통표고리(token ring) 언급한바와 같이 통표고리체계는 원래 차페꼬임쌍선도선을 리용하여 실현되였다. 이것은 후에 전통적인 비차페꼬임쌍선도선을 리용하는데 적용되였다. 통표고리망은 매 워크스테이션을 집선기에 련결하기 위하여 두개의 쌍선을 쓴다. 한 쌍선은 자료를 전송하는데 쓰이며 다른 쌍선은 자료를 수신하는데 쓰인다. 차페꼬임쌍선케블들은 통표고리망을 련결하기 위하여 두개의 쌍선을 포함하고 있고 전화전송을 위하여 추가적인 쌍선을 포함할수 있다. 이것은 통표고리망환경으로 하여금 음성과 자료를 반송하는데 같은 배선을 리용할수 있게 한다.

UTP케블은 전형적으로 4개의 쌍선을 포함하고 있는데 통표고리망에서는 두개의 쌍선만 리용된다. 통표고리망을 실현하는데서는 일반적으로 매체이음부로서 한개의 9핀 D–외피접속기를 리용한다. 지금은 비차페꼬임쌍선을 적응시켜 D–외피나 더 널리 보급된 RJ–45자료쟈크를 리용할수 있다. 현대적인 통표고리망기판은 두 이음부를 다 지원한다. RJ–45쟈크를 가지지 못하는 낡은 통표고리망기판은 완전저항정합변압기를 리용하여 비차페꼬임쌍선망에 아직은 련결할수 있다. 이 변압기는 100Ω완전저항의 케블로부터 그 카드가 기대하는 150Ω완전저항으로 변환된다.

케블취약성

케블에는 어느 정도 직접적인 취약성이 있다. 그것은 원래 이것이 물리적매체이기때문이며 결과적으로 직접간섭이나 직접적손상 같은것은 다시 배선할것을 요구한다. 그렇지만 무선통신의 출현과 함께 망우에서 아무런 지식도 없이 자료를 엿볼수 있게 되였다.

간섭

간섭은 어떤 장치가 의도적이든 아니든 케블을 통하여 전기적신호의 흐름을 와해시키거나 방해하는 위치에 놓일 때 발생한다. 자료는 전기적성질을 리용하여 케블을 따라 흐르며 자기마당이나 다른 전기마당에 의하여 변화될수 있다. 이것은 결과적으로 케블우에서 전체 신호의 손실이나 자료의 변경을 빚어 낸다. 자료의 변경은 일반적으로 자료의 손실을 가져 온다. 간섭은 기계류, 마이크로파장치들 그리고 지어 형광등장치에 의해서도 발생될수 있다.

이와 같은 정황을 처리하기 위하여 엇바뀌는 배선경로조정체계(전기도관을 포함하여)를 전개하며 케블배선의 위치선정을 돌보기 위하여 특수한 설비들을 배치하는것이다.

추가적으로 차페나 케블을 보호하기 위하여 금속피복을 포함시켜 신호의 손실위험을 감소시키는 배선방법이 개발되였다. 빛섬유케블은 신호전송에 빛을 리용하기때문에 이 문제로 피해를 받을 일은 없다.

케블절단

이것은 그 어느것보다 더한 망불법행위의 원인인것 같다. 이 경우에 신호는 케블이 물리적으로 절단된 결과에 차단된다. 설비를 옮기거나 케블근처를 파헤칠 때 절단되는 일이 일어 날수 있다. 공중교환봉사를 제공하는 통신회사들은 케블을 처음으로 설치할 때 망여유회선을 설치하는 방법으로 이런 사고를 처리한다. 그들은 전체적인 통신손실이 생길 경우를 줄이기 위하여 추가적으로 고장방지대책이 포함되게끔 자기의 망을 설계한다. 일반적으로 LAN관리자는 이런 근심을 하지 않는다. 그의 관심은 비루스로부터 그리고 부정확하게 취급되여 정보를 잃게 되는 결과가

일어 나는것으로부터 탁상형콤퓨터를 보호하는데 초점을 둔다. LAN관리자는 또한 사무환경의 돌발적인 손상과 봉사인원이나 건설자들로 하여 케블이 절단되는 일이 일어 날수 있다는것을 명심하여야 한다. 긴급대책과 수복대책계획을 가지지 못하면 자기의 지위를 위험에 빠뜨리게 된다.

케블손상

케블의 손상은 정상적인 마모로부터 생길수 있다. 케블련결동작이 지나치게 오래면 케블플라그와 쟈크우의 접속두가 파손될수 있다. 케블은 파도한 구부림이나 당기기로 인해서도 저절로 손상될수 있다. 이것은 망에서 때때로 통신중단을 일으킬수 있으며 믿을수 없는 통신에로 이끌어 갈수 있다. 케블파손은 적절한 설치기술을 통하여서와 기술설명서에 알맞는 조작을 효과적으로 하기 위하여 로출된 케블에 대한 정기적인 검사를 수행함으로써 감소시킬수 있다.

도청

도청은 전기신호를 도청하려는 케블결에 어떤 장치를 놓고 도청한후 그것을 외부전송매체우에서 류사한 신호로 다시 변환할 때 일어 난다. 이것은 도청을 알아 차리고 있기때문에 본래의 수신기와 송신기없이 정보를 알아 볼 능력을 가진 허가되지 않은 사용자가 제공한다. 이것은 이써네트가 직렬케블을 가지고는 더 쉽게 실현할수 있으나 빛섬유케블을 가지고는 훨씬 더 어려운데 왜냐하면 빛섬유케블을 로출시켜야 하기때문이다. 빛섬유케블의 바깥피복이 손상되면 그의 특성이 변경되여 현저한 신호손실이 빚어 지게 된다.

물리적공격

대부분의 망장치들은 물리적측면에서 공격을 받기 쉽다. 그것은 그 어떤 진지한 망설계자가 케블함, 케블도관 기타 물리적보호장치를 리용하여 장치들의 물리적보안을 취하는데 적당한 관심을 돌리게 될것이기때문이다. 물리적접근을 하면 공격자가 거의 아무것이나 할수 있다는것은 알려 진것이다. 그렇지만 많은 경우 공격자는 충분한 시간을 가질수 없다. 만일 공격자들이 자기의 공격과 접근획득을 개시하는데 시간이 필요하다면 그들은 론리적접근이나 망에 기초한 접근을 리용할것이다.

론리적공격

많은 망요소들은 망을 거쳐 접근할수 있다. 결과적으로 이 모든 장치들은 비법접근

을 거절할수 있게 정확히 구성되여야 할것이다. 이 장치들에 대한 침입이나 공격을 식별하기 위하여 추가적인 예방, 검출 그리고 대응장치들을 설치해야 할것이며 기관안에 있는 해당 감시대리점들에 그것을 보호하게 하여야 한다.

요 약

오늘날 망작업환경에 대하여 정보보안전문가들이 알아야 할 문제들은 많다. 그렇다고 해서 망기술자들이 안전한 해결책을 설계하는데 도움이 되게끔 모든 성분혹은 물리적전송방법전체를 리해해야 한다는것은 아니다. 그렇지만 이것은 그들이 무엇에 대하여 이야기하는가에 대한 지식과 망이 각이한 매체선택권을 가지고 구성되는 방법에서의 차이에 대한 지식, 고유한 위험이 무엇인가에 대한 지식을 요구한다. 그렇지만 각이한 망매체와 위상구조들이 있음에도 불구하고 위험요소들이 있는한 그것들사이에는 상당한 정도의 공통성이 있다. 만일 설계(즉 망수준의 암호화)안에 망수준의 보호가 고려되지 않았다면 보안기반의 그 어디엔가 그것을 포함시키는것이 필요하다.

망설계조와 보호전문가들은 자료의 보호와 무결성에 대한 관심이 망전반에 걸쳐 유지되는것을 담보하는데 밀접한 관계를 가져야 한다.

제6장. 유선 및 무선물리층보안의 문제점

제임스 트룰라브

망보안에 대한 문제는 보통 OSI–7계층모형의 상위층에 관한 문제이다. 그렇지만 인터네트상에서 오가는 자료통보문내용의 정상적인 보호이외에도 망의 물리적보안과 관련한 중요한 문제점들도 있다. 지어 방화벽안쪽에 있는 기업소망도 비법접근에 대하여서는 취약점을 가지고 있을수 있다.

기성유선망은 동선련결이든 빛섬유련결이든 관계없이 여러가지 수단에 의하여 도청을 당한다. 또한 침투적인 도청수법은 아니지만 결코 과소평가할수도 없는 망을 배회하는 방법들도 있다. 무선망형성이 추가적특성들을 가지게 됨으로 하여 물리적망보안은 약화되게 된다. 새로운 기술들이 출현하기때문에 물리적보안의 약화로 하여 회사정보가 손실될수 있는 가능성들을 구체적으로 따져 보아야 하며 위험성을 약화시킬수 있는 조치들도 강구하여야 한다.

침입탐지와 직접배선식감시와 같은 자동화된 보안조치들외에도 망관리절차를 세밀히 조직한다면 물리적보안을 개선할수 있다. 망설계를 정확히 하는것은 응당한 수준의 보안을 달성하는데서 매우 중요하다. 유선망에서 리용되는 조치들외에도 암호화를 리용하여 무선망들을 철저히 보호하여야 할것이다.

유선망위상구조의 기초

국부망을 구성해 본 사람이면 누구든지 망배선과 케블결선에 대한 기초적인 리해는 다 가지고 있다. 현대적인 LAN은 거의 례외없이 이써네트별형망이다. 개별적인 케블들이 중앙적인 능동집선기로부터 매 워크스테이션, 망인쇄기, 봉사기 혹은 경로기와 련결되여 있다. 오늘날의 기술수준에서 이 능동집선기들은 교환기능, VLAN(가상LAN)려과기능, 단순3계층경로조정과 같은 추가적인 기능들을 수행하기도 한다. 일부 경우에 이러한 장치들의 구성과 호상결선을 일정하게 달리하면 망의 물리적보안이 달라 질수도 있다.

망요소들의 구성방식을 그림 6－1에 보여 주었다. 그림 6－1에서는 사용자 대 집선기 그리고 집선기 대 집선기간의 표준적인 결선방식과 교환집선기가 망의 중심에 놓여 있는 결선방식을 보여 준다. 우에서 제시된 3개의 VLAN들은 부서가 서로 다른 사용자들을 리론적으로 구획하여 준다. 하나의 VLAN의 총적인 목적은 여러 그룹의 사용자들을 서로 갈라 줌으로써 그 사용자들이 일정한 응용프로그람들에 접근하지 못하게 하거나 서로의 자료들을 보지 못하게 하는것이다. VLAN들은 원래 도해로 표시하기 어려우며 따라서 물리층보안처리문제에서 다소 복잡하다. 흔히 자립형경로기들은 VLAN들사이의 자료경로를 서로 련결시켜 주며 방화벽을 통하여 인터네트를 비롯한 외부와 련결시켜 주는데 쓰인다. 이른바 3계층교환기는 이 경로기의 비WAN적기능들을 실제적으로 수행할수 있지만 일부 종류의 WAN경로기는 싸이트밖의 자료들을 인터네트와 같은 외부에 련결시키는데도 필요할수 있다.

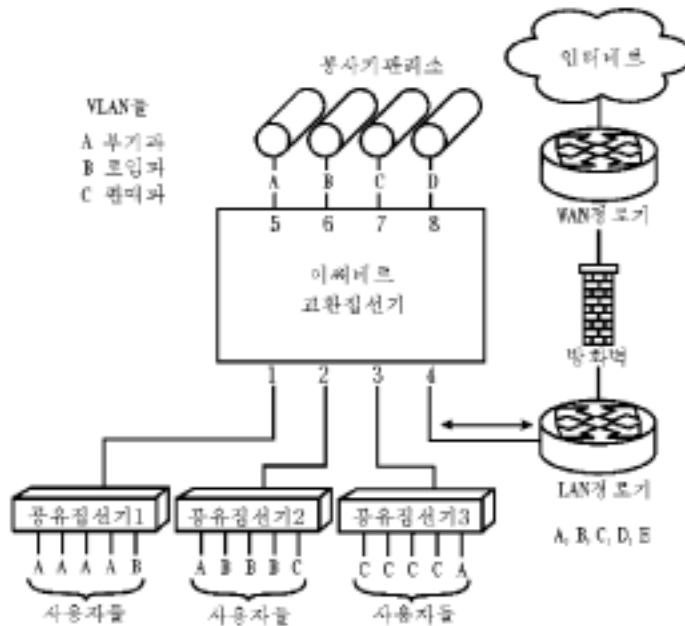



그림 6－1. 공유, 교환 및 경로조정된 련결을 가진 망의 위상구조

이 장에서는 이러한 망의 매 구성요소들의 물리층보안문제와 각 요소들사이의 실제적인 호상배선에서의 물리적보안문제들을 다룬다.

공 유 집 선 기

이써네트망위상구조의 원래 개념은 공유된 동축매체를 일정한 간격으로 중도에서 따서 워크스테이션들을 련결시키는것이였다. 이 매체의 매 길이를 토막이라고 하였으며 가능하면 그 토막에 반복기나 망다리를 련결하여 다른 토막들을 련결할수도 있었다. 매 토막에 련결된 국들은 신호가 없는가를 알아 본 다음에야 송신을 시작하며 그 매체에서 충돌요소(두 국이 같은 시간에 송신하는것)가 없는가를 감시하였다. 이 하나의 토막(혹은 중계기들로 련결된 여러 토막들의 묶음)은 충돌령역으로 간주되는데 이 령역내에서 그 어느 곳에서 충돌이 일어 나도 그 전체 령역에 영향을 미친다. 그러나 실제적으로 기본 동축선 혹은 그 어떤 련결송수신기, 련결케블, 접속구나 망대면부기판(NIC)들에 그 어떤 결함이 있어도 그 전체 토막에서는 교란이 일어 난다.

이 단일한 결함에 의한 고장의 효과를 극복하기 위한 한가지 방도는 중계기나 망다리들의 수를 늘이는것이다. 공유집선기를 설치하면 물리적케블의 결함으로 생기는 망고장을 줄일수 있다. 동축케블을 쓰는 이써네트망에서는 이 공유집선기를 다중포구반복기라고 불렀는데 이 것은 공유집선기의 기능들을 정확히 표현한것 같다. 일반적으로 10Base–T라고 부르는 꼬임쌍선케블 이써네트가 새로 출현함으로 하여 망결선보안이 더

강화되였다. 이러한 결선구조를 리용하면 결함이 있는 결선상태들을 알수 있으며 집선기에서 결함 있는 련결점들을 정확히 고립시킴으로써 충돌령역을 잘 보호할수 있다. 꼭 같은 형태의 공유망환경들은 10Base–F, 100Base–T, 100Base–FX, 100Base–SX(고속이써네트), 1000Base–T, 1000Base–TX, 1000Base–FX, 1000Base–SX(기가비트이써네트)에서도 가능하다.

그러나 공유집선기는 본질적으로 볼 때 자료교환을 위한 전송매체의 일부로 볼수 있다. 공유된 망에서 사적비밀에 대한 보장은 각국들의 호상협동에 의해서만 실현된다. 자료파케트들은 하나의 목적 및 원천 주소를 가지고 공유망에서 교환된다. 자료파케트들은 보낼 곳과 원천주소를 가지고 공유망에서 송신되는데 규약에 의하여 매 워크스테이션마디점들이 고유목적지주소를 가진 파케트들만 《기다리》게 되여 있다. 반대의 견지에서 보면 하나의 워크스테이션은 자기에게로 보내진 전송량만 오기를 기다리며 자기에게 할당된 주소를 원천주소로 하여 공유망에 자료파케트들을 보낸다. 정확한지.

실천에서는 망엿보기도구라고 부르는 정교한 망감시장치들을 그 어떤 공유망에 련결하며 매 개개의 전송파케트들을 보는것은 가능하다. 이 감시장치들은 매우 비싸고 (US$10,000~25,000) 성능이 전문화된 장치로서 리론적으로는 망침입을 제한하게끔 되여 있다. 그러나 성능이 훨씬 낮으며 덜 정교한 파케트탐색쏘프트웨어들도 쉽게 구입할수 있으며 그것들(PDA를 포함한)은 임의의 워크스테이션우에서도 가동할수 있다. 이렇게 되면 물리적보안문제가 상당히 복잡해 지는데 그것은 비법적이든 아니든 련결된 모든 망장치들이 공유LAN상의 모든 전송량들을 실지로 다 훔쳐 볼수 있기때문이다.

강제식엿보기도구들뿐아니라 워크스테이션도 비법적으로 망자원들에 간단히 접근할수 있다. 실례로 여러가지 망조작체계(NOS)환경에서는 합법적인 사용자에게만 허용된 망자원들에 누구나 쉽게 접근할수 있다. Microsoft회사의 보안결함들은 통과암호프로파일로부터 시작하여 NetBIOS에 이르기까지 그리고 능동통제구조로부터 시작하여 문제성 있기로 유명한 전자우편 및 열람기에 이르기까지 문건들에 매우 잘 반영되여 있다. 비법적으로 정보채취를 하는 우연적인 침입자가 쓸수 있는 프로그람들은 수없이 많다.

공유집선기환경에서 물리층보안에 관심을 돌려야 할것은 망자원에 접속된 워크스테이션들에 대한 물리적접근을 제한하는 문제이다. 대부분의 경우 이러한 워크스테이션에 대한 물리보안통제는 극상해야 시동통과암호, 망접속통과암호, 화면보호프로그람의 통과암호의 사용, 콤퓨터설비를 물리적으로 안전하게 건사하는것 그리고 물리매체보안에 국한되여 있다. 대부분의 콤퓨터시동루틴, 망접속, 화면보호프로그람 등을 쓰면 워크스테이션을 사용하지 않을 때 접근을 통제하고 보호할수 있다. 이 통과암호들은 개별화되여야 하며 자주 바꾸어야 한다.

망에 워크스테이션들을 추가하며 집선기를 다른 망장치들에 련결하는 절차들은 문건으로 잘 만들어 놓아야 하며 그 실현작업은 해당 권한을 부여 받은 전문인원들에 의하여 수행되여야 한다. 추가, 이동, 변경 등에 대한 문건도 잘 구비해 놓아야 한다. 또한 물리적인 망결선과 배선에 대해서는 외부기관의 검열을 정기적으로 받음으로써 망의 무결성이 담보되도록 하여야 한다. 이 검사외에도 워크스테이션들을 자체로 감시통제하는 망도구들과 스크립트들을 리용함으로써 모든 망결선장치들이 공개되고 승인을 받으며 망침입에 쓰일수 있는 그 어떤 쏘프트웨어도 없도록 하여야 한다.

교환집선기는 물리적보안을 확장시킨다

공유망의 기본적인 보안상 결함은 망을 횡단하는 모든 파케트들이 그 충돌령역안에 있는 모든 워크스테이션들에 가닿을수 있는 점이다. 사실상 충돌령역에는 수백개의 워크스테이션들이 있을수 있다. 교환집선기라고 하는 특별한 형태의 집선기를 리용하면 집선기의 자료처리량을 몇배로 늘일뿐아니라 보충적인 보안조치를 강구하는것으로도 된다.

교환집선기는 하나의 OSI 2계층장치로서 한 파케트의 목적지매체접근조종(MAC)주소를 조사하고 그 MAC주소장치가 있는 해당 교환기포구토막에만 그 파케트를 골라서 중계한다. 다른 말로 말하면 한 파케트가 그 어떤 포구로부터 들어 왔는데 포구 3에 있는 알려 진 MAC주소 X_1로 가게 되여 있다면 그 파케트는 직접 포구 3에 련결되여 보내지며 그 어떤 다른 나가는 포구에는 나타나지 않는다. 이 과정을 그림 6－2에서 설명한다. 교환기는 본질상 다중포구 2계층망다리로서 자기에게 련결된 모든 장치들의 MAC주소의 상대적인 위치들을 판정하여 처리된 매 파케트에 해당한 목적포구에로의 림시경로(목적 MAC주소에 기초하여)를 형성하여 준다. 이 처리는 대체로 《배선속도》로 진행된다. 포구들사이에 동시결선경로도 조성될수 있는데 그렇게 되면 공유망한계이상으로 처리률을 효과적으로 높여 준다.

교환집선기들은 흔히 간단한 물리적보안장치로 사용되는데 그것은 교환집선기들이 포구들을 고립시켜 파케트전송에 참여하지 못하게 하기때문이다. 전체 망이 교환식결선이 되여 있는 경우에는 이런 식의 보안이 좋다. 그러나 교환집선기들은 아직도 공유집선기보다 더 비싸며 그림 6－1에서 보는바와 같이 망들은 대부분 교환기 대 공유집선기위상구조를 리용하고 있다. 이것이 사용자집단들사이 그리고 일정한 망자원들사이를 격리시키는 하나의 조치로도 되지만 그렇게 되면 그 공유집선기에 련결된 한 사용자는 그 집선기에 련결된 다른 사용자에게 보내는 모든 파케트들을 볼수 있게 된다.

교환집선기상에서의 합법적검사와 감시는 공유집선기에서보다 훨씬 더 어렵다. 례를 들어 포구 7(그림 6－2)에 련결된 엿보기도구는 포구 8에서 포구 3으로 보내오는 파케트를 볼수 없다. 그 엿보기도구는 분명 자체의 MAC주소를 가져야 교환기가 그것을 인식하고 이 두 마디점들사이에 그 어떤 파케트도 통과하지 않게 될것이다. 이 문제를 일정하게 해결하기 위해서는 일부 집선기들에 포구거울화(port mirroring)라고 하는 기능이 필요하다.

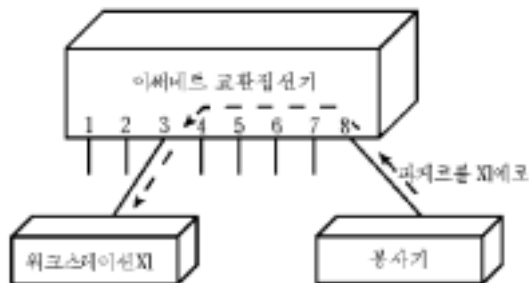



그림 6－2. 이써네트교환집선기의 동작

포구거울화라는 기능을 쓰면 선정된 포구에 모든 전송자료를 복사하여 주는 공유형 청취포구를 교환기상에 림시적으로 만들어 놓을수 있게 된다. 혹은 공유집선기를 포구 3이나 포구 8에 림시적으로 끼워 넣어 매 포구에 해당한 전송자료들을 볼수도 있다. 공유집선기가 있는 망의 일부분인 어느 한 포구에 실수로 거울화를 해놓는 경우 이것은 그 망에 하나의 보안상 위험으로 될수 있다. 특히 거울화해 놓는 포구가 우연히도 봉사기나 경로기결선에 리용되는 경우 특히 그 리용은 심각한바 그것은 이 장치로는 수많은 사용자들로부터 오는 자료를 볼수 있기때문이다. 교환식망에서의 보안리용을 극복하기 위해서는 포구거울화를 림시적인 고장퇴치기법으로만 리용하며 교환집선기의 운영을 정기적으로 감시하여 포구거울화가 되지 않도록 해놓는것이 좋다. 혼합형공유/교환식망에서 계층이 VLAN들을 쓰면 일정하게 마음이 놓이는 경우도 있다. 또한 같은 부서에서 전용적으로 쓰는 집선기들에 사용자들이 물리적으로 접근하지 않도록 함으로써 다른 부서의 자료들을 그 누가 내탐하지 않도록 하는것도 중요하다. 이렇게 되는 경우는 매 부서준위의 공유집선기들이 웃 준위의 교환식집선기에 련결되여 아마 VLAN에 의한 격리가 보장되는 경우일것이다. 관리자들은 통과암호관리를 엄격히 실행하며 교환기관리대면부에 대한 접근도 철저히 통제하여야 한다. 망보안에서 가장 우심한 위반현상은 기정값통과암호를 수정하지 못하는것과 통제통과암호를 정기적으로, 체계적으로 갱신하지 못하는것이다.

VLAN은 허위보안을 제공한다

망보안의 개선을 위하여 가장 흔히 리용되는 기능의 하나는 가상LAN구성기술이다. VLAN들은 계층 2나 계층 3에서 실현될수 있다.

계층 2에 속하는 VLAN에는 자료교환에 필요한 MAC주소목록이 포함되여 있으므로 관리하기가 상당히 힘들다. 다른 형태인 계층 1/계층 2에 속하는 VLAN들은 다른 VLAN들에 교환기의 물리적인 포구들을 배당한다. 여기에서 주의하여야 할것은 교환기포구에 련결되여 있는 모든 장치들이 그 VLAN에만 제한되여 있다는것이다. 따라서 공유집선기 1(그림 6－1을 참조)에 련결된 모든 사용자들은 교환집선기포구 1의 VLAN에만 속하게 될것이다. 이것은 망설계에서 하나의 우점으로 되며 보안을 상당히 높일수 있다.

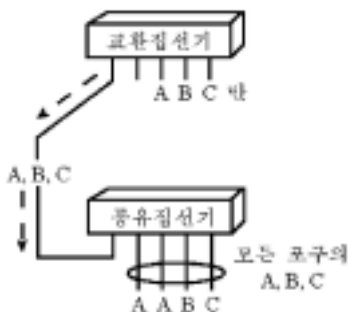



그림 6－3. VLAN A, B 및 C 교환집선기와
공유이써네트집선기를 통한 작용

여기에 계층 2에 대한 허위가 있다. 계층 2 VLAN은 계층교환망이나 혼성공유/교환망의 다른 모든 사용자들로부터의 파케트들을 격리시키지 못한다. 혼성망에서 모든 VLAN들은 그림 6−3에서 보여 준것처럼 임의의 공유집선기우에 있을수 있다.

따라서 공유집선기 2우에 있는 임의의 사용자는 VLAN에는 관계없이 그 집선기우에 있는 임의의 정보흐름을 엿볼수 있다. 포구에 기초한 계층 2 VLAN에서 관리자는 VLAN의 매개 포구에 접속되여 있는 모든 사용자들이 해당 포구로부터 나오는 혹은 해당 포구로부터 나가는 임의의 자료를 볼수 있도록 하여야 한다. 그러나 그렇게 할수 있는 유일한 방도는 매 사용자를 그 자신의 교환기포구에만 접속시켜 주어야 하는데 그렇게 되면 VLAN이 가지고 있는 편리성이 없어 지며 추가적인 설치의 복잡성이 생기게 된다. MAC에 기초한 VLAN은 여전히 다른 사용자들로 하여금 공유집선기나 거울화된 교환집선기상에서 파케트들을 엿볼수 있게 한다.

계층 3 VLAN은 실제적으로 높은 수준의 규약부분망이다. MAC주소외에도 인터네트규약(IP)자료를 가지고 있는 파케트들은 원천주소와 목적주소를 가진다. 부분망이라고 하는 IP주소들의 부분모임에는 많은 주소들이 련속적으로 담겨 져 있다. 표준적으로 IP장치들은 기준주소와 부분망마스크(부분망주소범위를 규정하는)들을 통하여 부분망들을 인식한다. IP규약묶음은 같은 부분망안의 주소가 아닌 자료교환을 가려 낸다. 계층 3에 해당하는 경로기는 부분망사이의 접속을 할수 있게 한다. 기술적으로 두개의 장치들은 같은 부분망내에서 서로 《말을 주고받을수 있는》 IP주소를 가져야 하거나 그 두개의 부분망들을 인식하는 경로기를 통하여 련결되여야 한다.

문제는 바로 서로 다른 부분망의 IP자료파케트들이 그 어떤 충돌령역내에서도 공존할수 있다는것 즉 동일한 공유집선기나 교환기련결상에서 존재할수 있다는것이다. TCP/IP규약은 자기장치에 해당하는 주소를 가지지 않는 파케트들은 그 어느것이든 무시해 버린다.

사실상 임의의 워크스테이션상의 엿보기 또는 훔쳐보기프로그람은 충돌령역안에 있는 모든 전송흐름에 대하여 IP주소에 관계없이 다 볼수 있다. IP전송이 아닌 경우에도 우의 사실이 그대로 성립된다. 비법적인 국이 전송흐름을 훔쳐 보지 못하도록 자원에 대한 물리적접근제한에 주의를 돌리지 않는다면 각이한 부분망들에 장치들을 배치하여 자료전송을 보호한다는것은 하나의 롱담에 불과하다.

VLAN/부분망에 교환기의 첨부

VLAN과 부분망을 가진 교환망에서 전적으로 교환기만 사용해도 상당한 정도의 보안대책이 세워 질수 있다. 사실상 이러한 방식은 많은 핵심망들에서 특정한 보호된 경로에 자료흐름과 자원이 흘러 들어 가지 않도록 제한하기 위하여 리용하는 방식이다. 자료에 직접 접근할수 있는 경우 그 싸이트의 물리적보안에 위험성이 조성된다. 물리적인 접속이 해당 장치들에만 국한되고 포구거울화를 하지 못하게 설정되여 있고 그 어떤 원격탐색(흔히 트로이목마라고 부른다.)프로그람들도 은밀히 가동하지 못하며 방화벽조치들이

확고히 서 있는 한 물리적계층에서 볼 때 망보호는 상당히 안전해 질것이다. 비법접근위험을 줄이는것은 물리적보안에 크게 달려 있다. 다음 부분에서 볼수 있는바와 같이 유선물리적보안은 매우 중요한 다른 하나의 문제로 된다.

유선물리적보안

유선물리적보안은 본질적으로 세가지 측면을 가지고 있다. 즉 합법적인 결선, 우발적인 신호의 전파, 유선물리적무결성이다. 첫번째 요구는 현존케블배선상태를 조사하고 모든 망이 정확히 배선되였는가를 확인하는것이다. 매국의 케블, 련결코드, 련결판, 집선기등에 일관성 있게 계통적으로 표식을 해두는것은 모든 망배선상태에 대하여 누구나 다 알게 하며 또 합법적인것으로 되게끔 하는데서 필수적인것이다.

매 케블들이 어떻게 련결되였는가, 해당 배선이 실지로 필요한가, 콤퓨터들의 위치가 변경되면 낡은 배선이 회수되는가. 콤퓨터가 없는 위치에 망배선을 위한 예비꽂개를 가지고 있는것보다 어리석은 일은 없다. EIA/TIA–596 A《원격통신경로 및 공간에 대한 상업적건설물표준》과 EIA/TIA–606 《상업적건물의 원격통신기반에 대한 관리표준》은 망배선 및 공간구성에 대한 배치, 규격, 표식달기에 대한 광범위한 안내지침을 주고 있다.

그외에 ANSI/TIA/EIA–568 B의 《상업적건물의 원격통신케블배선표준》이 권고하는 케블성능측정값들은 파일에 보관하여 정기적으로 그 측정을 반복하여야 한다. 리유는 단순하다. 자료흐름경로의 배선도중에 도청장치를 설치하면 많은 경우 케블성능이 그라프적으로 심하게 변화될것이다. 실례로 벽이나 천정에 숨겨 케블에 공유집선기를 끼우면 자료를 도청할수 있게 된다. 그러나 이렇게 하면 케블스캐너가 알려 주는 케블길이는 물론 다른 파라메터들도 달라 지게 된다.

망케블배선에는 두가지 형태 즉 4쌍의 동선으로 이루어 진 케블과 한쌍의 빛섬유로 이루어 진 케블이 있다. 둘다 은밀히 감시 당할수 있다. 동케블배선은 물리적접속이 필요하지 않기때문에 위험성이 더 크다. 잘 알려 진바와 같이 고속자료망배선에서는 2개 또는 그이상의 절연된 동선꼬임쌍선으로 전기적신호를 보낸다. 10Base–T 이써네트는 10MHz의 기본진동수를 가지며 신호성분은 그이상이다. 100Base–T 고속이써네트에서는 부호화기술을 리용하여 대부분의 신호성분주파수를 100MHz이하로 유지한다. 둘다 전자기마당을 산생하는데 그 전자기마당은 대체로 선쌍을 이루는 두 도체사이에 존재한다. 그렇지만 실지 에네르기의 일정한 량은 케블을 둘러 싸고 있는 공간으로 복사된다.

이 형태의 케블배선과 관련하여 주의해야 할 기본문제는 이 복사되는 신호가 일반라지오파수신에 장애가 되지 않도록 작아야 한다는것이다. 그렇다고 하여 그 신호가 너무 작아서 전달되지 못할 정도로까지 되여야 한다는것은 아니다. 사실 제3부류케블이 있는 곳이면 어디서든지 거기서 나오는 전자기신호를 더 잡을수 있다. 제5부류와 그이상의 케블들은 등급상으로만 더 좋은 케블일따름이다. 달리 말하면 그 케블은 전자적인 측면에서 《김이 새는》 호수처럼 배선 전 구간에서 약간한 량의 신호를 계속 흘리게 된다.

케블의 경로를 따라 임의의 곳에 수감기를 설치하면 자료신호를 잡을수 있다. 실지

로는(다행스러운 일이지만) 이보다 좀더 힘들기는 하다. 그것은 이렇게 하자면 기술이 매우 정교해야 되며 접근, 전력 그리고 적당한 수신점도 필요하기때문이다. 이밖에 쌍방향(완전2중)전송은 여러겹케블이 그러하듯이 두 방향으로 보내는 자료를 서로 차페한다. 이것은 물리적인 직접접속에서보다는 보통자료망에 대하여 적은 위협을 줄것이지만 그렇다고 하여 그 위협을 무시하지 말아야 한다.

빛섬유케블도청은 실행하기가 훨씬 힘든 문제이다. 동선배선에서와는 달리 빛섬유로 보내는 신호는 빛형태이고 유리섬유안에서 반송된다. 그렇지만 도청이 라체빛섬유나 호상 접속점에서 접근을 하게 된다면 신호에 뚫고 들어 가 도청할 방법은 있다. 빛의 대부분이 유리섬유를 따라서 세로방향으로 통과한다는것은 사실이다. 그렇지만 사람이 그것을 검출할 수단을 가지게 된다면 빛섬유의 측면벽을 통하여 극히 작은 신호량은 리용할수도 있다. 아마도 이 빛신호는 다자태빛섬유에서 더 잘 루출될것인바 거기서는 빛이 단일자태빛섬유에서와 같이 두께가 매우 가는 속심에 국한되지 않는다. 이밖에 빛섬유주행경로의 많은 호상접속점가운데서 어느 하나에 접근할수 있다면 누구든지 선을 따서 자료를 감시할수 있을것이다.

빛섬유케블구간들에는 련결부(patch)와 수평빛섬유케블쌍이 있어 거기에 달린 접속구들은 이음카드와 수평도관의 매 끌점들에 련결시킬수 있게 되여 있다. 이음접속구가 달린 케블의 매 경간들은 피동결합기(adapter라고도 부름)를 사이에 두고 서로 련결된다. 실례로 전형적인 빛섬유선들은 벽을 따라 워크스테이션을 련결할수 있는 콘센트에로 들어온다. 이 케블의 두 빛섬유선들의 끌에는 SC 혹은 한개의 새로운 소형요소접속구와 같은 빛섬유단자가 붙어 있다. 벽결선판에 있는 빛섬유접수기(adapter)에 그 련결단자들을 꽂은 다음 그 결선판은 콘센트함에 붙인다. 사용자케블 즉 련결선(patch cord)은 바로 그 빛섬유접수기의 바깥부분에 꽂아 설비와 련결한다. 만약 어떤 사람이 결선판에서 설비접속구들을 뽑아 그 빛섬유회선에 어떤 도청장치를 끼워 넣는데는 시간이 몇초밖에 걸리지 않을것이다. 그것은 결선판이 SC접속구와 같은 표준접속구들로 간편하게 구성되여 있기때문이다.

벽결선판에 쓰이는 빛섬유종단형태들이 일부 경우 호환성이 없음으로 하여 이러한 위험성들은 일정하게 감소되였다. 그렇지만 이것은 약간의 재간만 가지면 쉽게 극복할수 있는것이다.

직접 선을 련결하거나 망케블에 따들어 가는 경우 흔히 케블결선이 림시적으로 중단되여야 한다. 케블감시장치들을 쓰면 케블에서의 순간적인 결선중지상태를 탐지할수 있으며 그런 장치를 가지고서는 비법집선기를 통해 케블을 다시 련결하거나 그 망에 새로운 결선을 할수도 있게 된다. 이러한 전문케블감시장치들은 일어 나는 모든 사건들을 다 보고하고 기록함으로써 관리자는 케블결선체계상에 그 어떤 비정상적인 상태가 조성되는 경우 인차 알수 있게 되여 있다.

보안사고는 현실적으로 일어 나며 따라서 그에 대해서는 미리 예상하는것이 좋다. 방화벽뒤에 침입검출체계를 설치하여 내부 및 외부의 보안상 문제점들을 방지하여야 한다. 그렇게 되면 내부망에 대한 비법접근을 검출하는 가장 효과적인 도구로 될것이다. 침입검출체계의 기능에는 규약의 상위층들에 대한 감시는 물론 물리층에 대한 경보체계와 보고체계도 포함되여 있어야 한다.

무선물리층보안

무선망장치들은 본질상 목적을 가지고 자기의 주변에 무선신호를 내보낸다. 물론 합법적인 장치들만 그 무선신호를 수신하게 되여 있지만 도청을 막는것은 불가능하다. 망주소화와 무선망《이름달기》를 한다고 해도 그것이 우연한 사용자가 무선망에 들어 오지 못하게 하는데서는 효과적일수 있지만 실제적인 도움은 크게 주지 못한다.

무선자료송신을 쉽게 감시하지 못하게 하는 유일한 방도는 자료의 암호화이다. 현재 판매중에 있는 많은 무선LAN장치들은 지금 유선등가사적비밀보장(WEP:Wired–Equivalent Privacy)을 표준기능으로 제공하고 있다. 이 기능은 64비트암호화표준으로서 수동열쇠교환을 리용하여 무선망대면부기판(WNIC)과 접근점망다리(Access point bridge)(이것은 유선망에 접속한다.)사이의 신호를 개별화한다. 이것은 그 이름이 보여 주는것처럼 높은 수준의 보안으로는 되지 못하며 LAN케블결선상에서와 같은 수준의 사적비밀보장을 제공할따름이다.

일부 WNIC들이 128비트암호화와 같은 보다 긴 암호화알고리듬을 리용하는것은 추가적인 보안조치의 하나로 될수 있을것이다. 그렇지만 이 암호화체계에는 관리상 문제점이 하나 있어서 열쇠들을 철저히 보관하여야 예견한 수준의 사적비밀보장의 무결성이 담보될수 있다.

흔히 쓰는 쎌방식의 무선체계와 같은 무선 WAN접속에는 다른 하나의 보안상 문제점이 있다. 현재 효과적인 암호화기법을 쓰는 체계들은 얼마 없으므로 수신력과 복호화장치가 있으면 그 누구든지 이러한 망들에 쉽게 접속할수 있게 되여 있다. 따라서 이러한 망체계에서 비밀통신을 진행하려면 강력암호화수준의 SSL을 반드시 리용하여야 한다.

결 론

완성된 망보안계획에는 망의 물리층에 대한 고려사항도 포함되여 있어야 한다.물리적보안을 위한 공고한 토대를 마련하는데서 망설계를 잘하는것은 근본적의의를 가진다. 망실천에서는 교환집선기를 리용하고 자료의 경로들을 구체적으로 계획화함으로써 기밀자료들이 불필요하게 로출되는 일이 없도록 하여야 할것이다. 망관리자는 망케블배선체계에 대한 정확한 기록을 보존하고 상시적으로 갱신함으로써 합법적접근을 문서화하며 모든 이동과 추가사항들을 반영하도록 하여야 할것이다. 또한 보안향상을 위하여 망과 케블에 대한 감시를 적극적으로 할수 있는 장치들도 설치할수 있다. 뿐만아니라 망케블에 대한 검열을 정기적으로 진행함으로써 모든 결선상태에 대한 무결성과 합법성을 담보하도록 하여야 한다. 련결점들도 정기적으로 반복하여 조사하며 변화된 상태를 구체적으로 조사하여야 한다. 무선LAN접속에서는 적어도 WEP표준에 맞는 암호화수법을 리용하여야 하며 강력한 암호화체계도 사용하여야 한다. 마지막으로 정보보안관들은 각 계층에 대한 정기적인 보안검열을 진행하여 내부보안감시사업들을 호상 확인하여야 할것이다.

제7장. 망경로기의 보안

스티븐 에프 블랜딩

경로기는 자료통신망동작의 중요한 요소로 된다. 이 장에서는 망경로기의 능력과 망을 관리하는데 리용할수 있는 보안특성에 대하여 서술하고 있다. 경로기는 국부망, 광지역망에서 그리고 망봉사제공자와 인터네트에 외부적접속을 하기 위하여 리용된다.

경로기의 하드웨어 및 쏘프트웨어 구성요소

경로기는 그자체가 각이한 능력을 제공하며 대면부와 함께 있음에도 불구하고 하드웨어와 쏘프트웨어구성요소의 핵심모임을 포함하고 있다. 핵심하드웨어요소들은 CPU, RAM, 비휘발성RAM, ROM, 플래쉬기억기 그리고 I/O포구를 포함하고 있다. 그림 7—1에서 이것들에 대하여 륜곽적으로 보여 주었다. 형태에 따라 경로기의 요소들은 각이하게 설정될수 있으며 그것들은 장치의 조화로운 전반동작에 결정적인 작용을 하며 경로기보안특성을 지원한다.

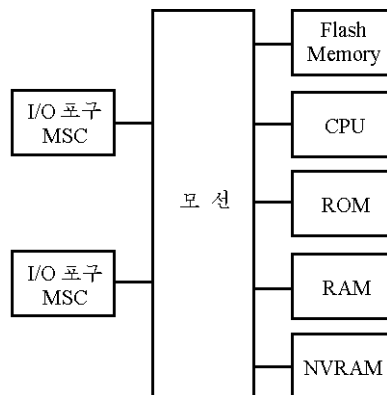



그림 7—1. 경로기하드웨어의 기본구성요소들

- **중앙처리장치** PC들과 더 큰 콤퓨터체계의 전형적인 중요한 요소로 알려 져 있는 CPU는 망경로기에서도 역시 중요한 요소로 된다. 극소형처리장치인 CPU는 경로기의 처리능력에 직접 련관되여 경로기의 조작체계를 구성하는 명령들을 수행한다. 조종탁이나 텔네트(Telnet)접속을 통하여 입력된 사용자지령들도 또한 CPU에 의하여 처리된다.
- **읽기쓰기기억기** RAM은 경로기안에서 여러가지 많은 기능을 수행하는데 리용된다.

RAM은 또한 파케트의 완충(장치가 동작할 때), 경로기설정파일을 위한 기억제공, 경로조정표의 유지에 리용되며 또한 공통대면부에서 통신흐름의 혼합으로 인하여 직접 내보낼수 없을 때 파케트대기렬을 위한 구역제공에 리용된다. 동작기간에 RAM은 주소변환규약(ARP: Address Resolution Protocol)정보를 기억하기 위한 장소를 제공하는데 이것은 경로기에 접속된 국부망의 전송능력을 높여 준다.

- **비휘발성RAM** 경로기의 전원이 꺼질 때 RAM의 내용은 지워 진다. 경로기의 전원이 꺼질 때 비휘발성RAM(NVRAM)의 내용은 유지된다. 경로기의 설정파일의 복사본이 NVRAM에 기억될 때 전원고장으로부터의 회복은 훨씬 빨라 진다. 결과 설정파일의 기억을 위하여 개별적인 하드디스크나 플로피장치를 보존할 필요는 없어 진다. 마모나 하드구동기와 같은 구성요소의 가동은 경로기하드웨어고장의 일차적원인이다. 그러므로 이러한 움직이는 구성요소들을 없앨 때 수명은 훨씬 더 길어 진다.
- **읽기전용기억** 경로기의 체계기판우에 있는 읽기전용기억(ROM)소자에 들어 있는 코드는 전원투입을 진단한다. 이 기능은 PC들이 수행하는 전원투입에 대한 자체검사와 류사하다. 망경로기에서 OS쏘프트웨어는 ROM에 있는 초기적재프로그람에 의해서도 적재된다. 쏘프트웨어의 품질은 경로기의 일부 형태에서 ROM소자를 제거하고 재배치하는 방법으로 갱신할수 있다. 한편 각이한 기술을 리용하여 조작체계를 기억하고 관리할수도 있다.
- **플래쉬기억** 지울수 있고 프로그람화할수 있는 ROM의 한 형태가 플래쉬기억이다. 경로기의 마이크로코드와 OS이미지는 대다수의 경로기우에 있는 플래쉬기억기에 보관될수 있다. 플래쉬기억기의 비용은 전 기간에 소자갱신에서 얻어지는 절약비로 쉽게 보상될수 있다. 왜냐하면 그것은 소자의 제거나 교체가 없이 갱신될수 있기때문이다. 기억용량에 따라 여러개의 OS이미지를 플래쉬기억장치에 기억시킬수 있다. 경로기의 플래쉬기억기는 OS를 다른 경로기에 옮겨 보관하게 하는 일반파일전송규약(Trival File Transfer Protocol)에도 리용될수 있다.
- **입/출구 포구** 파케트들이 경로기로 들어 오고 나가는 접속부가 I/O포구이다. 매체의 특수한 형태에 대한 물리적대면부를 제공하는 매체특정변환기는 매 I/O포구에 접속된다. 매체의 형태에는 이써네트 LAN, 통표고리 LAN, RS–232 및 V.35 WAN이 있다. 자료파케트들이 포구와 변환기를 거쳐서 지나갈 때 매 파케트는 CPU에 의하여 처리되여 경로조정표에 따라 파케트를 어디로 보낼것인가를 결정하여야 한다. 이 처리를 처리교환방식이라고 한다. LAN으로부터 자료가 접수됨에 따라 파케트가 RAM에로 이동될 때 두번째 층의 머리부들은 제거된다. 파케트의 출구포구와 교갑화하는 수법은 이 과정에 의하여 결정된다.

처리교환방식의 변종을 고속교환이라고 부른다. 여기에서 경로기는 목적지IP주소와 다음 마디점대면부에 대한 정보를 담고 있는 완충기억을 관리한다. 고속교환에서 경로기는 경로표에서 이미 얻은 정보를 보관하여 완충기를 설정한다. 이 도식에서 특수한 목적

주소로 가는 첫번째 파케트는 CPU로 하여금 경로표를 참고하게 한다. 개별목적지주소를 위한 next–hop대면부에 관한 정보가 얻어 지고 그 고속교환완충기에 기억된후에는 이 목적지주소에 보낼 새 파케트를 이 경로표에서 더는 찾아 보지 않는다. 결과 경로기 CPU에 대한 부하가 실질적으로 감소되며 교환파케트에 대한 경로기수용능력은 훨씬 더 빠른 속도로 생기게 된다. 일부 형태의 보다 높은 성능의 종단경로기모형은 고속교환의 발전된 변종을 고려한 특수한 하드웨어의 특성이다. 경로기의 형태에 상관없이 완충기는 대면부접합의 목적주소를 획득하고 기억하는데 리용된다. 일부 발전된 특징을 가진 경로기도 원천IP주소와 웃층의 TCP포구를 얻는다. 이러한 형태의 교환방식을 망흐름교환이라고 한다.

경로기의 초기화

경로기는 장치에 전원이 투입될 때 미리 정해 진 일련의 조작들을 수행한다. 경로기의 사전설정에 따라 추가적인 조작들이 수행될수 있다. 이 조작들은 경로기의 안정성에 이바지하며 그의 적절하고 안전한 기능수행에 필요한것이다.

경로기가 수행하는 첫번째 기능은 전원투입검사 또는 POST라고 하는 여러 공정의 진단검사들이다. 이 검사들은 경로기의 처리장치, 기억장치 및 대면부회로의 동작을 확인하기 위한것이다. 전원이 투입된 상태에서 수행되는 기본기능들과 함께 이 기능도 그림 7－2에 제시되였다.

흐름도에 따르면 POST과정이 완료되자마자 초기적재프로그람은 조작체계 OS를 주기억에로 초기화한다. 이 과정의 첫 단계는 경로기설정등록기를 검사하여 OS이미지위치를 결정하는것이다. 이미지는 ROM, 플래쉬기억 혹은 망에 있을수도 있다. 등록기설정은 OS의 위치를 가리킬뿐아니라 조종탁말단이 진단통보문을 연시하는가 그리고 경로기가 조정판건반우에 있는 중지건의 입구에 어떻게 반응하는가 하는것들을 포함하여 다른 건기능들을 정의하기도 한다. 설정등록기는 초기적재마당을 가리키는 마지막 4bit를 합하여 16bit값이다. 경로기의 설정파일의 위치는 초기적재마당에 의하여 식별된다. 초기적재등록기가 가장 일반적인 설정인 2로 설정되는 경우에 경로기는 초기적재지령에 관한 설정파일을 탐색하게 될것이다. 이 설정이 발견되지 않는 경우에 경로기는 플래쉬기억기로부터 OS이미지를 적재하게 된다. OS이미지가 플래쉬기억기에 없으면 경로기는 OS이미지가 요청하는 TFTP를 방송주소에로 내보내게 된다. 그러면 이미지는 TFTP봉사기로부터 적재될것이다.

일단 등록기설정과정이 완결되면 초기적재프로그람은 경로기 ROM에 이미지를 적재한다. OS이미지가 지금 적재된 상태에서 이전의 설정파일이 보관되여 있는가 하는것을 결정하기 위하여 초기적재프로그람으로 시험한다. 그다음 이 파일이 ROM에 적재되여 실행된다. 이때 경로기는 동작할수도 있게 된다. 만일 이 파일이 NVRAM에 기억되지 않으면 설정대화는 OS에 의하여 실행된다. 이 설정대화는 조종탁조작자에게 제기된 미리 규정된 질문의 순서렬인바 이 질문순서렬은 설정정보구축을 위하여 완성되여야 한다. 그다음 설정정보는 NVRAM에 기억된다.

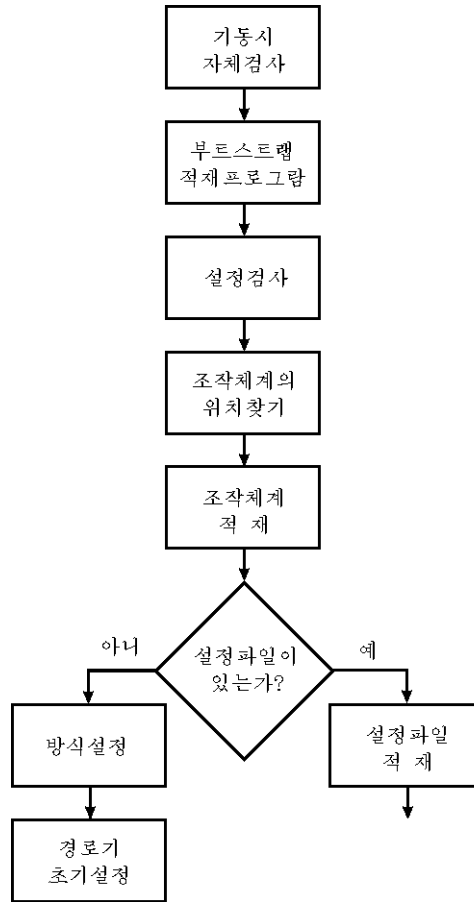



그림 7−2. 경로기의 초기화

련이어 일어 나는 초기화과정에 이 설정파일판은 NVRAM으로부터 복사될것이며 RAM에 적재될것이다. 경로기의 통과암호회복기간에 설정파일의 내용을 우회하기 위하여 설정등록기는 NVRAM내용을 무시하라는 지령을 받을수 있다.

조작체계이미지

이미 언급한바와 같이 초기적재프로그람은 설정등록기의 설정에 기초하여 OS이미지를 찾아 본다. OS이미지는 다음과 같은 기능을 수행하는 여러 루틴들로 구성되여 있다.

- 사용자지령수행
- 각이한 망기능지원
- 경로조정표갱신
- 완충기공간관리를 포함하여 경로기를 통하여 자료전송을 지원하기

이 OS이미지는 기억기의 낮은 주소공간에 기억된다.

설정파일

설정파일의 역할은 경로기초기화과정에서 간단히 론의되였다. 경로기관리자는 이 파일을 설정하는데 대하여 책임이 있으며 이 파일은 OS에 의하여 해석되는 정보를 포함하고 있다. 설정파일은 OS안에 구축된 각이한 기능수행을 책임진 관건적인 쏘프트웨어구성요소이다. 가장 중요한 기능의 하나는 접근목록표에 대한 정의와 그것들이 OS에 의하여 각이한 대면부에 어떻게 정의되는가에 대한 정의이다. 이것은 경로기를 통과하여 파케트흐름에 영향을 주는 조종의 정도를 확립하는 중요한 보안통제기능이다. 다시 말하여 OS는 보안통제를 확립하는 설정파일에 기억되여 있는 접근조종목록명령문들을 해석하고 수행한다. 설정파일은 조종탁조작자가 그것을 보관할 때 NVRAM기억기의 높은 주소공간에 기억된다. OS는 그다음 그것에 접근하여 NVRAM의 보다 낮은 기억주소공간에 기억된다.

경로기의 자료흐름조종

경로기가 자료흐름을 어떻게 조종하는가를 리해하는것은 이 망장치의 전면적인 작용에 대한 관건적인 문제로 된다. 설정파일에 기억된 정보는 경로기를 거쳐 자료가 어떻게 흘러 갈것인가를 결정한다.

우선 처리되여야 할 프레임의 형태는 매체대면부(이써네트, 통표고리, FDDI 등)에서 이전에 입력된 설정지령에 의하여 결정된다. 이 지령들은 하나 혹은 그이상의 조작속도와 대면부를 완전히 규정하는 기타 파라메터들로 설정되여 있다. 경로기는 도착하는 자료의 프레임형식을 검증하고 지원해야 할 대면부의 형태를 인식한후에 출구용프레임을 전개한다. 출구용프레임들은 그 대면부를 통하여 혹은 다른 대면부를 통하여 형성할수 있다. 경로기가 제공하는 중요한 조종특성은 정확한 순환여유검사(CRC)를 리용하는 능력이다. CRC의 특성은 대면부가 경로기에 알려 져 있기때문에 수신된 프레임우에서 자료의 무결성을 검사하는것이다. 또한 정확한 CRC가 계산되고 경로기에 의하여 매체에 배렬된 프레임에 덧붙여 진다.

경로조정표입력자료들을 나타내는 방법은 NVRAM에 있는 설정지령들에 의하여 조종된다. 이 입력자료들은 정적경로조정, 자료흐름우선권경로조정, 주소결합 그리고 파케트목적주소대면부의 경로조정 등을 포함한다. 정적경로조정이 이루어 질 때 그 경로기는 다른 경로기와 경로조정표입력자료들을 교환하지 못한다. 우선권경로조정에 의하여 하나 혹은 그이상의 우선권대기렬로 자료가 흐를수 있는데 거기서 높은 우선권을 가진 파케트는 우선권이 낮은 파케트를 앞서 지나간다. IP주소와 그에 대응하는 MAC주소사이의 결합을 기억하는 기억기의 범위는 ARP완충기에 의하여 표시된다. 파케트의 경로로 될 목적주소대면부도 역시 경로조정표의 입력자료들에 의하여 정의된다.

자료가 경로기안으로 지나갈 때 여러가지 결심채택조작과정이 발생한다. 례를 들어

자료파케트의 목적주소가 LAN이고 그리고 주소결정이 요구되면 경로기는 ARP완충기를 리용하여 MAC전송주소와 나가는 프레임의 목적지를 결정하게 될것이다. 만일 캐쉬에 정확한 주소가 없으면 경로기는 필요한 MAC주소를 결정하기 위하여 ARP파케트를 형성하고 내보내게 된다. 일단 목적지주소와 교갑화방법이 결정되면 파케트는 밖으로 나가는 대면부포구로 송달될수 있게 준비된다. 우선권규정에 따라 파케트는 송신완충기안으로 전송되기에 앞서 우선권대기렬안에 놓일수 있다.

경로기설정

경로기와 결합된 보안관리범위를 론의하기에 앞서 먼저 경로기설정과정을 리해하여야 한다. 이 과정은 기본설정고찰에 대한 리해, 지령해석기, 사용자조작방식, 특권조작방식 및 설정지령의 여러가지 형태들에 대한 본질적인 리해를 가져야 한다. 다음으로 접근보안목록과 보안관리의 암호조종기능을 서술한다.

경로기설정설비

경로기설정설비를 리용하여 경로기에 이름을 할당하고 직접접속과 가상말단통과암호를 할당한다. 일단 설정이 끝나면 조작자는 설정을 접수하라는 재촉을 받게 된다. 설치설정처리기간에 조작자는 매 규약과 대면부에 관한 여러가지 특정한 파라메터를 입구할수 있게끔 준비되여야 한다. 준비중에 조작자는 설치된 대면부의 형태와 리용할수 있는 목록에 정통하여야 한다.

경로기설치지령들은 미리 확립된 설정입력자료들을 조사하는데 리용될뿐아니라 허용되는 통과암호를 변경시키는데도 리용된다. 조작자는 경로기조종탁포구에 허용되는 지령을 입력하여 통과암호를 규정하여야 한다. 이 지령은 경로기의 동작환경을 변경시키는 특정한 수행지령들에 접근할수 있게 한다. 또한 허용되는 안전통과암호라고 하는 다른 통과암호는 접근보안을 제공하는데 리용될수 있다. 이 통과암호는 허용되는 통과암호와 같은 목적으로 쓰이지만 허용되는 안전통과암호는 설정파일에서 암호화된다. 결과 설정이 조종탁우에 연시될 때 허용되는 안전통과암호의 암호화된 판본(version)만이 사용될수 있다. 따라서 허용되는 안전통과암호는 경로기설정이 이미지를 얻는다고 하여 로출되지는 않는다. 허용되는 통과암호(또한 가상말단, 보조품 그리고 조종탁포구)를 암호화하기 위하여서는 봉사통과암호의 암호화지령을 리용할수 있다. 이 암호화기술은 그닥 위력한것은 아니며 공통적으로 쓸수 있는 통과암호해독쏘프트웨어를 통하여 쉽게 절충될수 있다. 그러므로 허용되는 통과암호는 설정파일에 충분한 보안을 제공하는데 리용되여야 한다.

지령해석기

경로기는 지령해석기를 리용하여 조작자가 입구하는 경로기지령들을 해석한다. 해석기는 지령부분을 검사하고 요구되는 조작을 수행한다. 지령해석기에로의 접근을 위하여

조작자는 정확한 통과암호에 의하여 경로기에 접속되여야 한다. 이것은 설치과정에 이루어 지게 된다. 조작자는 두개의 서로 분리된 지령해석기수준이나 접근수준을 리용할수 있다. 이것은 사용자지령과 특권지령을 의미하는데 그 매개는 서로 다른 통과암호로 설정되여 장비된다.

- **사용자조작방식** 사용자조작방식은 오직 경로기에 접속될 때만 얻어 진다. 이 접근수준은 조작자로 하여금 개방접속의 연시, 말단파라메터의 변경, 론리적접속의 이름설정 그리고 다른 호스트에 접속하기와 같은 기능을 수행할수 있게 한다. 이것들은 모두 중요하지 않은 기능들로 간주된다.
- **특권조작방식** 특권지령들은 예민하고 중요한 조작들을 수행하는데 쓰인다. 례를 들면 특권지령해석기는 조작자로 하여금 말단잠그기, 특권명령의 인입과 차단, 설정정보입력을 수행할수 있게 한다. 표 7-1은 일부 특권방식지령들의 한개 목록을 보여 주고 있다. 사용자방식에 쓰일수 있는 모든 지령들은 또한 특권방식에도 쓰일수 있다.

사용자방식의 명령들은 그 목록에 포함되지 않았다.

표 7-1 특권방식의 지령들

지 령	기 능
Clear	기능들을 다시 설정한다.
Configure	설정방식을 입력한다.
Conect	열린말단을 접속한다.
Disable	특권명령을 무효화한다.
Erase	플래쉬기억이나 설정기억을 소거한다.
Lock	말단을 잠근다.
Reload	끄고 다시 시동하는것을 수행한다.
Setup	설정지령설비를 가동시킨다.
Telnet	Telnet대화를 개방한다.
Tunnel	턴넬접속을 개방한다.
Write	가동하는 설정을 기억기에 쓴다.

특권방식조작은 경로기를 설정하는데 리용된다. 이 방식에 처음으로 들어 갈 때에는 통과암호가 요구되지 않는다. 허용되는 통과암호지령은 특권방식에 련이어 계속되는 접근을 위한 통과암호를 할당하는데 리용될것이다.

설정지령들

설정지령들은 경로기를 설정하는데 리용된다. 이 지령들은 네 부류로 나누어 진다. 즉 전체적인것, 대면부, 회선 및 경로기부분지령들로 분류된다. 표 7－2는 경로기설정지령목록을 보여 주고 있다.

표 7－2 경로기설정지령들

지 령	리 용
Write terminal	RAM에 있는 현재의 설정정보를 연시한다.
Write network	RAM의 현재설정정보를 TFTP를 거쳐 망봉사기와 공유시킨다.
Write erase	NVRAM의 내용을 소거한다.
Configure network	망봉사기로 이전에 창조된 설정정보를 적재한다.
Configure memory	NVRAM으로 이전에 창조된 설정정보를 적재한다.
Configure terminal	조종탁으로써 수동으로 경로기를 설정한다.

전체적인 설정지령들은 체계전체의 파라메터를 규정하며 접근표들을 포함하게 한다. 대면부지령들은 LAN 혹은 WAN대면부의 특성을 규정하며 한개 대면부명령이 그다음에 놓인다. 이 지령들은 망을 개별적포구에 할당하고 대면부에 요구되는 특수한 파라메터들을 설정하는데 리용된다. 회선지령들은 직렬말단회선연산을 변경하는데 리용된다. 끝으로 경로기부분지령들은 IP규약파라메터들을 설정하는데 리용되며 경로기지령이 리용된 다음에 쓰인다.

경로기접근조종

이미 언급한바와 같이 경로기와 특권지령리용에 대한 접근조종은 통과암호의 리용을 통하여 확립된다. 이 지령들은 표 7－3에 제시되여 있다.

표 7－3 경로기접근조종지령들

지 령	기 능
Enable password	특권 EXE방식접근은 이 통과암호에 의하여 설정된다.
Enable secret	MD5암호화를 리용한 허용되는 안전한 접근은 통과암호에 의하여 설정된다.
Line console 0	회선조종탁의 접근은 이 통과암호에 의하여 설정된다.
Line vty04	텔네트접속접근은 이 통과암호에 의하여 설정된다.
Sercvice password encryption	연시지령을 리용할 때 이 지령은 그 통과암호연시를 보호한다.

경로기접근목록

경로기접근목록의 리용은 접근보안조종의 행정관리에서 관건적역할을 한다. 경로기의 가장 중요한 보안특징의 하나는 망안에서 자료파케트흐름을 조종하는 능력이다. 이 특징을 파케트의 려과라고 하는데 이것은 원천 및 목적지 IP주소 그리고 리용되는 응용의 형태에 기초하여 망에서 자료흐름의 조종을 고려한다. 이 려과는 접근표를 리용하여 수행된다.

파케트에 들어 있는 정합기준에 기초하여 경로기를 거쳐 자료파케트가 흐르는것을 허용하거나 거절하는 명령문의 순서목록은 접근목록으로 정의된다. 접근목록에는 두가지 중요한 측면이 있다. 즉 한 측면은 접근목록명령문의 순서렬이나 차례이고 다른 측면은 접근표의 마지막에 하나의 절대적인 부정명령문을 리용하는것이다. 려과가 정확하게 되도록 하기 위하여 명령문은 접근표의 정확한 순서로 입력되여야 한다. 또한 명시적인 허가명령문들을 리용하여 자료가 암시적인 거절명령문에 의하여 기각되지 않도록 해야 한다. 명백히 허가되지 않은 파케트는 접근목록의 끝에 있는 무조건 《모두 거부》명령문에 의하여 기각될것이다.

경로기들은 프로그람화되여 파케트려과를 수행함으로써 각이한 종류의 많은 보안문제들을 처리할수 있다. 례하면 파케트려과를 리용하여 특수한 주소명령으로부터 시작되는 망작업에 텔네트대화파케트가 들어 가지 못하도록 할수 있다. 파케트들을 허용하는데 리용하는가 아니면 거부하는데 리용하는가 하는 기준은 파케트의 3층이나 4층머리부에 들어 있는 정보에 좌우된다. 접근목록들이 파케트들을 려과하기 위하여 4층이상에 있는 정보를 리용할수 없으므로 문맥에 기초한 접근조종(CBAC)이 리용될수 있는바 CBAC는 응용층에서의 려과가능성을 제공한다.

관리령역

관리령역은 워크스테이션, 봉사기, 망련결 및 단일한 관리집단에 의하여 유지되는 경로기와 같은 망장치들의 일반적부류의 하나이다. 경로기는 관리령역들사이의 경계로서 리용된다. 매개 관리령역은 자기자체의 안전방책을 가지고 있다. 결과 개별적인 령역은 자료망들사이에 제한된 접근을 가지고 있다. 대다수의 기관들에는 한개 관리령역만이 필요될것이지만 만일 서로 다른 보안방책이 요구된다면 개별적인 령역들이 창조될수 있다.

경로기들은 령역들사이의 경계로 리용되지만 또한 행정관리령역들을 접속하는데 도 리용된다. 경로기들은 회사망들의 두개 혹은 그이상의 행정관리령역들을 련결하는데 리용될수 있거나 회사의 행정관리령역들을 인터네트에 련결하는데 리용할수 있다. 모든 자료파케트들이 경로기를 통하여 흘러야 하며 경로기들이 지리적으로 분산된 싸이트들을 련결하는데 리용되여야 하기때문에 추가적인 설비나 쏘프트웨어를 요구할 필요는 없고 경로기가 파케트려과기능을 제공하기만 하면 된다. 정교하고 복잡한 보안을 하는 정확한 보안방책을 수행하기 위한 모든 기능을 망경로기가 제공할수 있다.

보안방책과 기타 경로기기능을 창조하기 위하여 씨스코회사(Cisco)가 리용하는 조작체계를 망결합조작체계(IOS: Internetwork Operating System)라고 한다. 조종탁조작자에 의하여

입구된 명령들은 IOS와 대면부로 접속한다. IOS는 이 명령들을 리용하여 경로기설정을 관리하고 기억기 및 대면부와 같은 체계하드웨어를 조종하며 그리고 파케트들의 이동과 경로조정 및 ARP표와 같은 동적정보를 구성하는것 등의 체계과제들을 수행한다. 이외에 IOS는 Windows, Linux 및 Unix 등 기타 조작체계들에서 볼수 있는 많은 특징을 가진다.

접근목록들은 또한 파케트려과와는 다른 기능들을 제공한다. 이 기능들에는 경로기접근조종, 경로기려과작용갱신, 파케트대기렬 및 수요에 의한 다이얼조종이 있다. 접근목록들은 SNMP 및 Telnet와 같은 기구를 통하여 경로기에로의 접근을 조종하는데 리용된다. 또한 접근목록들을 리용하여 망이 경로기려과갱신을 통하여 경로조정규약이라고 알려 지지 못하게 할수 있다. 파케트의 어떤 부류들은 접근목록들을 리용함으로써 다른 파케트부류들에 대한 우선권을 부여 받아 밖으로 나가는 각이한 대기렬들에 이 파케트형식들을 지정할수 있다. 마지막으로 접근목록들을 리용하여 다이얼접속기능을 리용하도록 파케트들을 정의함으로써 이 기능을 시동시킬수 있다.

파케트려과

앞에서 설명한바와 같이 접근목록의 기본기능은 파케트를 려과하는것이다. 려과는 망의 안전을 보장하는데서 하나의 중요한 기능이다. 여러가지 장치를 리용하여 파케트를 려과할수 있다. 파케트려과는 또한 방화벽내부의 하나의 공통적인 특징인데 방화벽안에는 망보안이 구축되여 내부의 신뢰성 있는 체계들과 외부의 신뢰성 없는 체계들사이의 접근을 조종한다. 어느 파케트가 경로기의 통과를 허용 받으며 어느 파케트가 경로기의 통과를 거부 당하는가 하는것을 파케트내부에 담겨 진 정보에 기초하여 결정하는것을 바로 파케트려과도구라고 한다.

관리자들은 파케트려과도구를 리용하여 경로기를 통과하기 위하여 파케트가 준수해야 할 일정한 기준들을 정해 놓는다. 지정된 해당 기준항목에 맞지 않으면 파케트는 통과를 거절당한다. 파케트가 거절도 되지 않고 허용도 되지 않는다면 그 파케트는 기존값에 의하여 거절된다. 이것을 암시적거절이라고 하며 오늘 산업에서 사용되는 공통적이며 중요한 보안특성의 하나로 된다. 언급된것처럼 암시적거절은 기존값으로 동작하지만 명시적허용에 의하여 무시될수도 있다. 파케트려과를 통한 다른 보안특성들은 제한성을 가지게 된다. 이 제한성들에는 무상태파케트검사, 정보검열제한성들, IP주소위장 등이 있다.

무상태파케트검사

접근조종목록이 어떤 파케트가 TCP/UDP대화의 일부분인가를 결정하지 못할수도 있는데 그 원인은 매 파케트가 마치도 단독적인 실체인것처럼 되여 검사 받기때문이다. ACK비트가 설정된 내향성TCP파케트가 실지 현존대화의 일부분인가를 결정하는 방도는 아직 없다. 이것을 무상태파케트려과(례하면 경로기가 현존대화의 상태나 지위에 대한 정보를 가지고 있지 못한다.)라고 부른다. 무상태파케트검사는 비문맥성접근조종목록에 의하여 수행된다.

상태표들을 리용하여 원천지주소, 목적지주소, 경로기와 자료들을 교환하는 포구들을

기록할수 있다. 들어 오는 파케트들이 검사를 받아 현재 진행중에 있는 대화의 부분인가를 확인 받지만 전통적인 접근목록은 어떤 파케트가 현존상위층대화의 부분인가 아닌가를 판별하는 능력은 못 가지고 있다. 접근목록을 리용하면 개별적인 파케트들을 검사하여 그것이 현존대화의 부분인가를 결정할수도 있겠지만 설정된 열쇠단어를 사용하는것이 기본이여야만 가능하다. 그러나 이 검사는 TCP대화에만 한정되여 있는데 그 원인은 UDP가 비접속형규약이며 현 접속상태를 보여 주는 기발이 규약의 머리부분에 전혀 없기때문이다. 또한 TCP대화에서는 이 조종이 위장수법에 의하여 쉽게 손상될수 있다.

정보검사한계

전통적인 접근목록들은 IP계층이상의 파케트정보를 검사할 때에는 검사능력이 제한되여 있고 제4계층이상의 정보를 검사하지 못하며 또한 안전하게 처리하는 능력이 없다. 확장접근목록은 제4계층의 머리부정보를 제한된 량만 검사할수 있다. 그러나 보다 최근의 접근목록기술에서는 일련의 갱신이 있다. 이에 대해서는 이 장에서 후에 보기로 하자.

IP주소위장하기

IP주소위장하기는 콤퓨터해커들이 망체계를 교란시킬 때 흔히 쓰는 망공격기술이다. 주소려파를 하여 IP주소위장하기를 없애려 하지만 이 주소위장하기는 남의 망주소를 자기망주소처럼 가장하여 자기가 보낸 파케트가 마치도 신뢰도가 있는 남의 콤퓨터가 보낸것처럼 위장한다. 주소위장을 하기 위하여 위장자는 초기TCP 3회주고받기(three–way handshake)를 하는 동안에 자기의 PC로부터의 SYN요청에 대한 대답으로 보내 온 초기순서번호로 추측하여야 한다. 도착지 PC는 SYN요청을 받자마자 SYN–ACK응답을 위장에 리용된 IP주소의 합법적소유자에게 보내온다. 결국 위장자는 응답을 절대로 받지 못하게 되여 있다. 따라서 위장자는 SYN–ACK파케트에 담겨 진 초기렬수자를 추측하여 공격자의 PC가 보낸 ACK에 정확한 정보가 담겨 주고받기과정이 완결되게 해야 한다. 바로 이 점에서 해커 즉 위장자는 성공적으로 망에 들어 간다.

공격자 즉 해커들이 그 누구에게 피해를 주는것이 목적이라면 망에 들어 갈 필요가 없다. 실례로 공격자가 나쁜 파케트를 어느 호스트체계에 보내여 그 호스트의 기능을 마비시키려 한다고 하자. 이런 형태의 공격을 흔히 봉사거부공격이라고 한다. 공격자는 단지 그 대상의 주소만 위장하면 되지 결코 그 대상과의 련결을 지을 필요는 없다.

표준접근목록

표준접근목록은 원천지IP주소에만 의거하기때문에 기능상 매우 제한되여 있다. 표준적으로 보면 이 표준접근목록은 응당한 수준의 보안에 필요한 세밀성을 보장하지 못한다. 그 세밀도는 1부터 99까지의 범위로 정의되지만 이름접근목록을 사용하여 그 등급을 정의할수도 있다. 이름을 접근목록에 리용함으로써 관리자는 일부 기입항목이 목록에서 삭제된후에 전체 목록을 다시 만들 필요가 없게 된다.

표준접근목록에서 매 기입항목은 매 파케트가 가공될 때 처음부터 끝까지 순차적으로 읽혀 진다. 그 파케트에 해당한 항목이 나타나면 나머지 접근목록내용은 무시된다. 결국 접근목록내용의 순서가 파케트의 해당 가공/경로조정에 매우 큰 역할을 한다. 만약 파케트와 접근목록사항사이의 일치가 없으면 목록끝에 도달할 때까지 파케트검사는 계속 진행되다가 결국 암시적인 《전체 거부》상태에 빠진다. 암시적인 전체 거부는 목록의 마지막에서 명시적인 전체 허용에 의하여 무시되여 암시적거부를 받은 임의의 파케트를 경로기를 통과하게 할수도 있다. 이것은 권고할만한 좋은 보안대책이 못된다. 가장 좋기는 허용된 파케트들을 위해서는 접근목록에 있는 명시적허용사항을 리용하고 일체 다른 파케트들에 대해서는 암시적전체 거부를 써서 거부하는것이다. 이렇게 하면 표준접근목록의 길이로 보나 복잡성으로 보나 상당히 안전한 실천으로 될것이다.

표준접근목록을 가장 효과적으로 사용할수 있는 경우는 가상말단접근을 제한시키거나 단순망관리규약(SNMP)접근을 제한시키며 망범위를 려과하려는 요구가 제기되는 때이다. 가상말단접근은 외부장치로부터 경로기로 원격접속할수 있는 능력을 말한다. 망내부에 있는 경로기에 원격접근하는것을 제한하기 위해서는 확장접근목록을 매개의 대면부에 적용할수 있다. 이것을 피하기 위해서는 표준접근목록을 적용하여(내부로 들어 오는) 단 하나의 장치로부터의 원격접근을 제한할수 있다. 또한 원격접근이 일단 실현되면 밖으로 나가는 대면부에 표준접근목록을 적용하여 모든 외향적접근을 제한할수도 있다.

표준접근목록은 또한 SNMP접근을 제한하는데도 리용할수 있다. 자료망에서 SNMP를 리용하면 봉사기와 경로기와 같은 망장치들을 관리할수 있다. SNMP는 망관리자들이 사용하는데 공동문자렬(community string)이라고 부르는 인증방식이나 통과암호를 사용하여야 한다. 표준접근목록은 또한 IP주소들을 제한하여 SNMP접근의 경로기통과를 허용함으로써 이 강력한 능력이 외부에 호출되는것을 훨씬 줄이게 한다.

표준접근목록은 특히 서로 다른 경로조정규약들사이에 재분배경로들이 있는 경우 망범위를 려과하기도 한다. 려과하게 되면 초기규약의 경로가 두번째 규약으로 재분배되였다가 다시 그 초기규약으로 돌아 오는것을 막을수 있다. 즉 표준접근목록을 사용하면 매 규약에 분배되게 된 경로들을 규제할수 있다.

확장IP접근목록

이름이 보여 주는것처럼 확장접근목록은 표준접근목록보다 더 강력하여 기능에서나 유연성에 있어서나 훨씬 좋다. 표준접근목록과 확장접근목록들은 둘다 원천지주소에 의하여 려과를 한다. 그러나 확장목록은 도착지주소와 상위계층규약정보에 의해서도 려과를 진행한다. 확장접근목록을 쓰면 봉사분야의 종류와 IP우선권에 의하여 려과를 할수 있다. 확장접근목록의 또하나의 특성은 사용기록이다. 접근목록의 제일 뒤에 있는 기입항목에 있는 LOG라는 열쇠단어를 사용하여 접근목록일치사항을 기록할수 있다. 이 기능은 선택사항이므로 설정해 주면 기록내용을 경로기가 지정하는 자료기지설비에 보낸다.

경로기접근목록을 리용하여 망보안방책을 수립할 때에는 몇가지 주요사항을 잊지 말아야 한다. 대면부와의 관계에서 접근목록을 배치할 때 표준접근목록은 될수록 도착지에 가깝게 놓아야 하며 확장접근목록은 될수록 원천지에 가깝게 놓아야 한다. 표준접근목록

은 원천지주소만 리용하여 해당 파케트를 거절할것인가 허용할것인가를 결정하기때문에 이 목록을 원천지에 너무 가깝게 배치하면 포함되여야 할 파케트들이 막혀 버리는 현상이 초래된다. 결국 확장접근목록들을 원천에 될수록 가까이 배치하는것은 이 목록이 표준적으로 원천지IP주소와 도착지IP주소를 다같이 리용하기때문이다.

강력한 보안방책에 반영되여야 할 내용은 또한 위장을 물리치기 위한 전략이다. 내향적접근목록에 《위장방지》접근목록항목들을 첨부하는것은 이러한 전략에 상당히 도움이 될것이다. 이 위장방지기입항목들을 리용하여 외부망의 원천지주소나 무효원천지주소를 가진 IP파케트들을 차단할수 있다. 무효원천지주소들의 실례로는 되돌림주소(loopback address), 다중전송주소(multicast address) 및 비등록주소들을 들수 있다. 위장은 해커들이 쓰는 매우 인기 있는 수법이다. 이런 가짜주소들을 사용하여 해커들은 추적을 받지 않으면서 공격을 진행한다. 보안관리자들은 파케트를 가지고 이 비법주소들을 사용하는 원천지를 추적해야 소용 없다.

동적접근목록

동적접근목록은 사용자인증과정을 통하여 접근목록에 동적인 빈자리들을 만들어 주는 능력이 있는 접근목록이다. 지금까지 설명한 모든 접근목록 즉 전통접근목록, 표준접근목록 및 확장접근목록에 다 이러한 목록기입사항들을 넣을수 있다. 사용자가 인증되고 사용자가 개시한 경로기에로의 Telnet의 접속조종을 경로기가 받은 다음에야 내부에 들어 오는 즉 내향성접근목록에 동적기입사항들을 만들어 넣을수 있다. 이 동적기입사항들을 리용하여 사용자콤퓨터의 IP주소로부터 오는 파케트들을 허용해 준다. 동적기입사항들은 유휴시간이 경과되거나 최고경과시간이 끝날 때까지 계속 남아 있다. 그러나 이 두 특성들은 선택적인 항목이며 일단 선택해 놓으면 다음번 경로기의 재적재과정이 있을 때까지 동적기입사항은 계속 활성상태로 있게 된다. 그러나 시간경과파라메터들을 리용하면 중요한 보안조치로 될수 있다.

동적접근목록을 사용하는것을 잘 계획하여야지 잘못하면 보안상 다른 제한성들을 발로시킬수 있다. 동적접근목록의 리용에서는 한종의 접근만 가능하며 각이한 준위의 접근은 제공되지 않는다. 또한 접속조종을 수립할 때 접속개시정보는 암호화됨이 없이 통과되기때문에 해커들이 엿보기도구들을 리용하여 이 정보에 접근할수 있게 된다.

결 론

망경로기보안은 기관들의 전반적보안계획의 사활적인 구성요소이다. 경로기보안은 보안전문가들의 항시적인 관심을 요구하는 복잡하고도 빨리 발전하는 기술이다. 지금까지 이 장에서는 기본적인 경로기보안특성들의 주요측면들과 그것들을 활용하여 비법공격을 막자면 어떻게 해야 하는가에 대하여 보았다. 공격의 위협과 공격의 첨단성이 계속 증가하고 있음으로 하여 앞으로 보안사업은 의심할바없이 개선되고 향상될것이다.

제8장. 무선인터네트보안

데니스 쎄이무어 리

인터네트의 초창기를 되돌아 보느라면 인터네트가 나오게 된 몇가지 리유에 대하여 다시 생각해 보지 않을수 없다. 그 리유의 일부를 본다면 다음과 같다.

- 전자적인 정보공유를 위한 광범한 통신매체를 제공하는것,
- 국부적인 가동중단에도 견딜수 있는 다중통로적인 망을 형성하는것,
- 각이한 제작자와 각이한 망사이에서 콤퓨터호상간 대화를 위한 방도를 제공하는것.

당시 상업과 보안(망사용을 위한 노력을 제외하고)에서는 그리 높은 수준의 요구가 제기되지 않았다. 초창기에 인터네트를 상업적목적에 리용할수 있다는 생각은 거의 없었다. 사실 인터네트를 리용하여 봉사를 하고 제품판매를 한다는것은 륜리상 어긋나는것으로 생각되였다. 상업활동의 요구와 그 보안상 요구는 최근 몇해사이에 보다 새롭게, 강하게 제기되고 있는 문제이다.

이와는 반대로 무선인터네트는 그 첫 시작부터 상업을 기본추동력으로 하여 설계되고 있다. 세계의 수많은 나라들과 기관들은 기업유지를 목적으로 수백만 지어는 수십억딸라를 들이밀어 기술시설, 전송주파수대역, 기술, 응용프로그람을 구매하고 있다. 일부측면에서 보면 이것은 새 천년기의 《질주경쟁》으로 된셈이다. 그렇다면 응당 여기서는 보안이 처음부터 결정적인 역할을 놀아야 한다. 자금의 이동이 있으니 보안도 그에 맞게 되여야 한다는것이다.

비록 무선산업이 아직은 유년기에 있지만 무선인터네트를 위한 장치개발, 기초시설개발, 응용개발은 전 세계적범위에서 급속히 확대되고 있다. 선견지명이 있는 사람들은 이 초기설계단계에서 보안이 응당 제 자리를 차지하여야 한다고 볼것이다. 이 장의 목적은 이 새로 태여나는 산업에서 반드시 제기되여야 할 주요보안상 문제점들의 일부를 명백히 밝히는것이다. 이 문제점들은 무선인터네트봉사나 응용을 도입하려는 기업이 기업보안 및 고객보호 그리고 새로운 보안인 무선인터네트에 대한 투자를 보호하는데서 응당 고려해야 할 우려들이다.

이 장에서 초점은 무릎형콤퓨터와 무선모뎀을 사용하는 인터네트를 분석평가하는것이 아니다. 나온지 몇해가 잘된 이 기술은 많은 경우 전통적인 유선인터네트접근의 확장일 따름이다. 이 장에서 초점을 맞추려고 하는것은 우선 LAN이나 인터네트Bluetooth도 아니다(100% 인터네트형도 아니며 몇개 장을 필요로 하는것이므로). 이 장이 기본적으로 설명하려고 하는것은 보통 PC보다 훨씬 낮은 콤퓨터능력을 가진것으로 원래 알려 진 이동전화와 PDA(개인휴대형정보처리기)와 같은 휴대형인터네트장치들이다. 따라서 이 기구들에서는 각이한 프로그람언어, 규약, 암호화기술, 보안안목을 가지고 여러가지 기술을 다루어야 할것이다. 그러나 크기가 작고 제한성이 있다 할지라도 이 기구들은 전자상업

거래와 현재 설계중에 있는 인트라네트관련응용으로 하여 정보보안에 상당한 영향을 미칠것으로 보인다.

누가 무선인터네트를 사용하는가

수많은 연구자료들과 예측자료들은 오늘 무선인터네트사용자의 수는 이제 곧 수백만의 유선인터네트사용자수를 훨씬 초과할것이라고 보고 있다. 이 예상수자는 매일 수천명씩 증가하고 있는 전 세계의 이동전화사용자수가 수백만이라는데 기초하고 있다. 만일 이 이동전화사용자 매 사람이 우선 전화를 통한 인터네트접근을 원한다면 사실 무선인터네트사용자수는 유선인터네트사용자수의 몇배를 넘을것이다. 바로 이 방대한 잠재력이 있음으로 하여 많은 기업들이 이 장성하는 산업을 독점해 보려고 수많은 자원과 투자를 아낌없이 투하하고 있는것이다.

무선인터네트는 아직 매우 청소하다. 무선전화로 인터네트에 접속하지 못하는 이동전화사용자들도 많다. 앞으로 제공할 봉사형태들에 대하여 두고 보자는 식의 태도를 가지고 있는 사람들도 많다. 무선인터네트접근을 하고 있는 대부분의 사람들은 초기도입자들로서 현재 이 무선인터네트봉사의 잠재력을 시험해 보는 사람들이다. 화면이 작고 매우 제한된 대역너비인데다 기타 문제들도 있는 무선기구들의 심각한 제한성으로 하여 유선및 무선인터네트사용자들의 대부분은 오늘 인터네트접근의 기본수단인 탁상형콤퓨터와 무릎형콤퓨터를 이 무선장치들이 대신하지 못할것이라고 인정할것이다. 무선장치를 가지고 《인터네트를 한번 쭉 훑는다는것》은 정말 실망할 정도로 힘든 일이라고 모두가 말한다. 무선인터네트사용자들중 대부분이 다음과 같은 실망감을 표시하였다.

- 인터네트에 접속하기에는 너무 속도가 느리다.
- 움직이기 시작하면 접속조종중간에서 접속이 끊기기 쉽다.
- 수자판에서 문장을 타자하기 시끄럽다.
- 분당으로 사용료를 지불하게 하면 무선인터네트가 사용하기에 비싸다.
- 무선장치들에는 그라픽스현시능력이 너무 적거나 없다.
- 화면이 너무 작아서 긴 문장을 읽으려면 내내 내려갔다올라갔다 해야 한다.
- Web싸이트훑기를 할 때 오유가 많다(주로 대부분의 Web싸이트들이 오늘날 무선인터네트와 호환성이 없기때문에).

이 글을 쓰는 당시 이 실망감을 주는 내용들중 하나의 례외적인 현상이 어느 한 나라에서 나타났다. 정보통신제공업체인 NTTDoCoMo(무선응용규약 즉 WAP에 대응되는)는 i–Mode라는 무선응용환경을 리용하여 무선인터네트가입자수에서 기록적인 장성을 보았다. 이 나라의 많은 사람들에게 있어서 무선전화를 리용한 접속은 인터네트와의 유일한 접근방법이다. 유선하부시설을 설치하기 곤난한 곳에서는 무선인터네트접근이 유선접근보다 훨씬 값이 눅다. i–Mode사용자들은 인터네트무선접속상태를 《언제나 직결》상태에

있을수 있게 하였으며 이동전화상에 천연색화면 지어 도형과 음악과 동화상까지도 펼칠 수 있게 되였다. 아마 무선인터네트와 관련한 이 성과는 정확한 요소가 주어 지면 무선분야에서 못할것이 없다는것을 례를 들어 보여 준것이라고 해야 할것이다.

어떤 응용이 가능할것인가

오늘의 무선기술의 실패요소들과 제한성들을 깨닫고 많은 기업체들은 자기식의 무선장치들과 무선봉사들을 설계하고 있는데 유선인터네트접근을 대신하자는것보다도 유선인터네트에서 할수 있는 봉사형태들의 확대판으로 전용봉사를 하자는것이다. 이러한 봉사형태들에서 뚜렷이 나타나는 장점은 휴대성정보접근의 편리성이다. 언제 어디서나 콤퓨터앞에 마주 앉지 않아도 주머니속에 가지고 다니며 인터네트봉사를 받을수 있게 된것이다. 사실 정보는 간명하고 휴대성 있으며 쓸모 있고 접근하기 편리해야 한다. 오늘날 설계되고 있거나 현재 가능한 무선봉사형태들은 다음과 같다.

- 이동전화를 사용한 직결물건사기를 할수 있다. 실지 상점에 들어 가서 상점의 물건값과 직결가격들을 비교도 할수 있다.
- 현 주식시세를 알수 있으며 가격정보, 무역권한부여, 종합정보 등을 어디서나 교환할수 있다.
- 은행거래를 하며 구좌정보를 받아 볼수 있다.
- 려행계획시간표를 받아 보며 예약할수 있다.
- 자기가 좋아 하는 새 소식과 날씨예보를 받아 볼수 있다.
- 최신추첨번호를 받을수 있다.
- 지급소포의 현 송달상태를 알아 볼수 있다.
- 전자우편을 《쉬지 않고》 계속 보내고받고 할수 있다.
- 재고명세, 고객명단 등과 같은 회사의 내부자료기지에 접근할수 있다.
- 지도상의 방향을 물어 보고 알수 있다.
- 사용자의 현 위치로부터 가장 가까운 ATM(자동현금입출기), 식당, 극장, 상점위치들을 알아 낼수 있다.
- 구급전화번호를 돌리면 구급봉사에서 요청자의 위치를 삼각점으로 추측할수 있다.
- Web싸이트를 열람하며 동시에 싸이트대표와 실시간적으로 이야기를 주고받을수 있다.

보다 새롭고 보다 혁신적인 봉사형태들이 현재 추진중이다. 새롭게 태여나는 기술들이 흔히 그러하듯이 무선봉사와 무선응용에 대해서도 희망과 함께 과장도 많으며 일부 사람들속에서는 위구도 없지 않다. 그러나 기술과 봉사형태들이 시간이 지남에 따라 성숙되여 어제날의 실험이 래일의 표준으로 될수도 있다. 인터네트는 이렇게 새롭게 나타

나는 진보의 커다란 모범이다. 무선인터네트의 발전도 꼭 같은 진화론적주기를 거칠것이며 그것은 더 빠른 속도로 나아갈것이다.

그러나 그 어느 기술과 마찬가지로 보안과 안전이라는 문제를 시작부터 설계에 정확히 포함시키지 않으면 그 기술자체의 평판과 전망에 오점을 남길수 있다. 바로 이러한 목적을 념두에 두고 이 장을 썼다.

무선인터네트는 포괄범위가 넓기때문에 그 보안도 포괄범위가 넓다. 이 장에서는 무선장치들에 대한 통신방법으로부터 시작하여 기술시설의 일부 구성요소들에 이르기까지 몇가지 부류에서의 무선인터네트보안문제들을 다룬다.

송신방법은 어느 정도 안전한가

몇해동안 사회적으로 인식된것은 상사식이동전화전송이 상당히 엿듣기 쉽다는것이다. 이것은 상사식이동전화가 리용되기 시작한 때로부터 알려 진 문제였다. 특수한 라지오스캔기구를 사용하면 엿듣기 쉽다. 이런 리유로 하여 많은 이동전화봉사제공자들은 수자식봉사를 추진하여 상사식을 줄이고 있다. 수자식이동전화전송은 표준적으로 볼 때 엿듣기가 보다 힘들다. 바로 이러한 꼭 같은 수자식전송방식에 새로운 인터네트봉사가 기초하고 있는것이다.

그러나 수자식쎌전송에는 하나의 방식만 있는것이 아니다. 사실 오늘날 무선전송방식에는 여러가지 각이한 방식이 있다. 실례로 어느 한 나라의 Verizon과 Sprint와 같은 봉사제공업체에서는 CDMA(코드분할다중접근)방식을 사용한다면 AT&T사에서는 주로 TDMA(시분할다중접근)방식을 쓰며 VoiceStream사에서는 GSM(지구적인 이동통신체계)방식을 리용하고 있다. Cingular 같은 다른 업체들에서는 지리적위치에 따라 하나이상의 방법들(TDMA와 GSM)을 사용하고 있다. 이 모든 방법들은 라지오주파수사용방식과 이 주파수들을 사용자에게 배당해 주는 방식에서 서로 차이가 있다. 이 장에서는 이 매개 방식들을 보다 구체적으로 설명한다.

이동전화사용자들은 무선인터네트접근에 관해서는 어떤 전송방법이든 관심도 없으며 실지 관심하려고 하지도 않는다. 대신 대부분의 사용자들은 자기가 좋아 하는 무선봉사제공자들을 선택하여 봉사에 가입한다. 봉사제공자가 어느 전송방법을 쓰는가 하는것은 일반적으로 사용자들에게는 잘 알려 지지 않을 정도로 투명하다. 그러나 봉사제공자에게는 이것이 완전히 다른 문제이다. 어느 방법을 리용하든지 그 방법은 그 기초시설과 상당한 관계가 있다. 실례로 라지오설비의 류형, 전송탑의 위치와 개수, 전송량, 가입자들에게 팔아 주는 이동전화류형 등은 모두 선택된 수자식전송방법과 직접적으로 련관되여 있다.

주파수분할다중접근(FDMA)기술

상사식이든 수자식이든 모든 쎌통신은 무선봉사제공업체가 구매하거나 그에 할당된 라지오주파수를 리용하여 진행된다. 매 봉사제공업체는 해당 정부로부터 라지오주파수대

역에 대한 사용허가를 구매한다.

상사식쎌통신은 대체로 주파수분할다중접근(즉 FDMA)기술이라고 부르는 방식에 기초한다. FDMA방법에서 매 봉사제공업체는 자기가 할당 받은 라지오주파수대역을 개별적인 주파수통로로 나눈다. 매 통로는 단방향통신대화를 지원하는 특정주파수이다. 매 통로는 10～30kHz의 폭을 가지고 있다. 정상적인 쌍방향전화대화를 위해서는 매 이동전화사용자에게 두개의 주파수통로가 차례져 하나는 송신에, 다른것은 수신에 쓸것이다.

매 전화가 두개의 통로(두개의 주파수)를 차지하므로 전용라지오스캔기구가 해당 주파수통로에 정확히 동조만 하면 진행중에 있는 상사형전화대화를 엿듣는것은 그리 힘든 일이 아니다. 암호화가 추가되지 않으면 상사형쎌통신에서는 사적비밀보호가 거의 불가능하다.

시분할다중접근(TDMA)기술

다른 한편 수자식쎌통신에서는 여러가지 코드화기법이 리용되는데 그 대부분이 상사형라지오주파수스캔에 견디여 낸다(주의 : 무선통신에서 단어 encoding은 encryption을 의미하지 않음. 여기서 encoding은 신호를 한 형태로부터 다른 형태로, 례하면 유선신호로부터 무선신호로 변환하는것을 의미함–역주).

이러한 수법들중의 하나가 바로 시분할다중접근 즉 TDMA이다. FDMA와 류사하게 TDMA는 라지오주파수를 여러개의 30kHz주파수(때로는 주파수반송파라고도 함)들로도 나눈다. 쌍방향통신을 하려면 이런 주파수통로가 두개 있어야 하는데 하나는 보내는 통로, 다른 하나는 받는 통로로 리용할수 있다. 그런데 TDMA에서는 보충적으로 매 주파수통로를 음성/자료통로라고 하는 3～6개의 시간소통로로 더 나누어 최고 6가지 수자식음성 및 자료회선이 같은 주파수상에서 진행되게 된다. TDMA봉사제공자들은 FDMA에 비해 볼 때 같은 시간에 더 많은 통화를 다룰수 있다. 이것이 동일한 하나의 주파수에서 매 시간소통로에 6개의 매 통화를 할당해 주기때문이다. 매 시간소통로(즉 음성/자료통로)는 지속시간이 대략 7ms이다. 이 시간소통로들은 빠른 순환으로 계속 순차적으로 송신된다. 해당 시간소통로에서 오는 정보들은 접수쎌기지국에서 신속히 추출하고 재조립하여 회화나 대화과정이 이어 지게끔 한다. 일단 시간소통로가 통화자에게 할당되면 통화가 끝날 때까지 그 통화자에게만 리용된다. TDMA방법에서는 매 사용자에게 전체의 한 주파수가 할당되는것이 아니라 다른 사용자들과 함께 공유하여 매 사람에게는 해당한 시간소통로가 차례질뿐이다.

이 장을 쓰는 현재도 TDMA전화대화나 자료흐름들은 무선공간으로 날아 가지만 이것들을 도청하였다고 하는 사건들이 공개된것은 많지 않았다. 도청하자면 아마 특수한 형태의 기구나 시험장치들이 있어야 할것이다. 짐작컨대 비법적으로 고쳐 만든 TDMA이동전화도 도청에 리용될 가능성이 있다.

그러나 그렇다고 하여 도청이 불가능하다는것은 아니다. 무선인터네트대화와 관련하여 이런 대화가 진행되는 전체 경로를 생각해 보라.

이동전화사용자가 인터네트Web싸이트와 통신하자면 무선이동전화에서 나오는 무선자료신호가 유선신호로 변환되여야 인터네트로 흘러 갈것이다. 유선신호로 된 그 정보는

해당 Web싸이트에 도착할 때까지 평문으로 인터네트를 종횡무진할것이다. 물론 무선신호자체는 도청하기 힘들지만 일단 유선신호로 변환되면 인터네트로 흐르는 모든 암호화되지 않은 통신들과 꼭 같은 도청위험성이 있다. 송신방법에는 관계없이 만약 극비정보를 인터네트로 보내려고 한다면 처음부터 끝에 도착할 때까지 그 대화전체를 암호화하는것이 필요하다. 암호화에 대해서는 후에 구체적으로 설명하겠다.

지구적이동통신체계(GSM)

다른 하나의 수자식전송방법이 바로 지구적이동통신체계(GSM)이다. GSM이라는 용어에는 전송방법만 담겨 져 있는것이 아니다. 이 용어는 각이한 GSM봉사로부터 실지 GSM설비와 기구자체에 이르기까지의 쎌전송방식체계전반을 의미한다. GSM은 주로 유럽나라들에서 사용된다.

일종의 수자식전송방법인 GSM은 TDMA의 변종이다. FDMA나 TDMA와 류사하게 GSM봉사제공자는 할당된 라지오주파수대역을 여러개의 주파수통로로 나눈다. 이때 매 주파수통로는 상당히 넓은 폭인 200kHz를 가진다. 다시 FDMA와 TDMA와 비슷하게 매 GSM이동전화는 두개의 주파수통로 즉 송신통로와 수신통로를 사용하게 된다.

TDMA와 같이 GSM도 매 주파수통로를 음성/자료통로라고 하는 시간소통로로 더 나눈다. 그러나 GSM에서는 8개의 시간소통로가 생겨 최고 8통화의 수자식음성 및 자료통신이 같은 주파수내에서 진행된다. TDMA에서는 일단 그 시간소통로가 통화자에게 배당되면 통화가 끝날 때까지 통화전기간 그 사용자에게 전용으로 리용된다.

GSM에는 보안을 강화하는 보충적인 특징들이 있다. 매 GSM전화에는 가입자신원모듈(SIM)이 있다. 이 SIM은 신용카드크기의 스마트카드나 우표크기의 소편과 보기에는 비슷하다. 사용할 때 이 외장SIM을 GSM전화에 끼워 넣는다. 이 스마트카드나 소편에는 가입자의 이동전화번호와 같은 가입자정보, 인증정보, 암호화열쇠, 전화번호목록, 가입자가 보관한 짧은 통보문들이 담겨 져 있다. 이 SIM은 꺼냈다넣었다 하는 외장식이므로 이것을 서로 다른 GSM이동전화에도 쓸수 있게 되여 있다. 전화를 쓸 때마다 가입자의 정보가 담긴 SIM을 쓰면 그 가입자의 전화로 된다. 즉 사용자의 신원은 특정한 어느 전화에 달려 있는것이 아니라 그 SIM자체에 달려 있다. 그러므로 전화번호를 바꾸지 않고도 서로 다른 GSM전화를 사용할수 있거나 가입자의 정보를 갱신할수 있다. 또한 다른 나라에 가면 그 나라의 GSM주파수가 달라도 GSM전화를 임대하여 쓸수 있다. 물론 이것은 매 나라의 GSM봉사제공업체들사이의 봉사호환성이 있어야 한다.

GSM전화는 SIM이 없이는 무용지물이므로 이 SIM은 인증도구의 기능도 수행한다. 일단 SIM을 전화에 끼워 넣으면 해당 SIM과 관련된 개인식별번호(PIN)를 입력하라는 통보문이 나온다(SIM이 PIN을 쓰게 되여 있는 경우). 정확한 PIN이 입력되지 않고서는 전화가 동작하지 않는다.

해당 전화기에 대한 사용자인증을 할뿐아니라 이 SIM은 또한 접속할 때 이 전화기를 전화망자체에 인증시키는 역할도 수행한다. SIM에 있는 인증(즉 Ki)키를 사용하면 전화기는 매 통화마다 봉사제공자의 인증쎈터에 인증을 등록한다. 이 과정은 문제-대응기법을 리용하는것으로 되는바 이것은 어떻게 보면 PC를 원격망에 접속할 때 통표카드를

쓰는것과 류사하다.

SIM이 들어 있는 키들은 인증외에도 또 다른 하나의 기능을 가지고 있다. SIM카드가 생성하는 암호화(즉 Kc)키를 쓰면 이동전화와 봉사제공자의 송신설비사이의 통신을 암호화함으로써 비밀성을 보장할수 있다. 이 암호화수법을 쓰면 이 두 지점사이에서 도청을 막는다.

TDMA와 류사하게도 이 GSM송신방법에서는 라지오주파수스캔기구로 도청하기 매우 힘들다. 하나의 주파수를 최고 8명의 사용자가 쓰므로 수자신호를 추출하기 어렵다. SIM카드를 리용하여 암호화까지 하면 GSM은 도청방지용으로 다른 한개의 보안층을 추가하는셈이다.

그러나 무선인터네트대화에 관하여 이야기한다면 이런 형태의 암호화는 말단 대 말단사이의 보호가 되지 못한다. 경로의 일부만 실지 보호될수 있다. 이것은 TDMA인터네트대화과정에서 이미 설명한것과 류사한 문제이다. 전형적인 무선인터네트대화는 무선경로도 있고 유선경로도 있다. GSM암호화는 다만 이동전화와 봉사제공자의 전송장소사이의 구간인 무선구간만 보호한다. 봉사제공자의 전송설비에서 인터네트Web싸이트까지의 유선인터네트의 구간은 평문으로 전송하는것으로 된다. 말단 대 말단암호화를 하면 전체 인터네트대화과정의 비밀은 보장될것이다.

코드분할다중접근(CDMA)기술

수자식전송방법에는 코드분할다중접근(CDMA)이라는 방법도 있다. CDMA는 확산스펙트르에 기초하고 있다. 이 기술은 라지오통신의 도청과 장애를 극복하기 위하여 군부가 오래동안 사용해 온 기술이다. Qualcomm회사는 이 CDMA확산스펙트르기술을 쎌방식의 전화에 도입한 주요개발자의 하나이다.

라지오주파수대역을 여러개의 좁은 주파수대역으로 혹은 시간소대역으로 나누지 않고 이 기술에서는 역시 주파수통로라고 하는 그 라지오주파수대역의 매우 넓은 부분을 그대로 리용한다. 그 주파수통로는 너비가 1.25MHz나 된다. 쌍방향통신을 위하여 매 이동전화는 송신과 수신에 각각 하나씩 두개의 이러한 넓은 CDMA주파수통로를 쓴다.

통신을 할 때 매 음성 혹은 자료대화는 처음에 여러 자료신호로 변환된다. 다음 그 신호들에 해당 통화자소속관계를 밝히는 고유코드로 딱지를 붙인다. 이 코드를 허위불규칙소음(PN)코드라고 한다. 매 이동전화는 매 대화시작때 기지국에서 새로운 PN코드를 할당 받는다. 이 코드화된 신호들은 매우 넓은 라지오주파수대역에 산포되여 전송된다. 통로너비가 매우 크기때문에 이 통신방법에는 해당 통화자소속표시인 PN이 붙은 많은 다른 대화들도 동시에 처리할수 있는 능력이 있다.

CDMA전화는 수신할 때 해당 PN코드를 리용하여 자기에게 오는 신호들만 골라 내고 나머지는 다 무시한다.

CDMA방식에서는 기지국과 통신하는 이동전화들이 모두 꼭같이 넓은 주파수들을 공유한다. 매 통화자를 구별해 주는것은(FDMA에서처럼) 사용하는 주파수도 아니며 해당 주파수내의 시간소통로로가 아니라(TDMA나 GSM과 같이) 바로 그 통화자에게 할당된 PN소음코드이다. CDMA방식에서 하나의 음성/자료통로는 고유PN코드가 붙은 자료신호

이다.

하나의 CDMA방식의 대화를 도청하는것은 힘들것이다. 그것은 그 수자식신호들이 매우 넓은 라지오주파수대역들에 널려 있기때문이다. 대화는 어느 한 주파수에만 머물러 진행하는것이 아니므로 스캔하기가 매우 힘들다. 또한 PN소음코드를 알지 못하고서는 그렇게 많은 주파수에서 해당 대화만 추출해 낸다는것은 불가능하다. 도청이 더욱 불리해지는것은 그 전체 통로대역에서 수많은 다른 통화자들이 동시에 대화를 하기때문이며 어느 한 통화를 도청하자면 굉장한 량의 소음을 극복해야 하기때문이다.

그러나 앞에서 본 다른 수자식통신방법들에서와 마찬가지로 CDMA이동전화를 리용한 인터네트대화도 도청하기 불가능한것은 아니다. 앞에서와 마찬가지로 CDMA수자식신호자체는 도청하기 힘들지만 이 무선신호들이 유선신호로 변화되기만 하면 유선신호들은 인터네트를 따라 가며 도청 당할수 있다. 말단 대 말단사이의 암호화를 하지 않고는 무선인터네트대화도 인터네트를 통한 암호화하지 않은 다른 통신들과 마찬가지로 위험하다.

기타 방법들

수자식전송에는 기타 방법들도 있는데 그 대부분은 이미 언급한것들의 파생형들이며 일부는 아직 개발중에 있다. 이 개발중에 있는것들을 가리켜 3세대 즉 3G전송방법이라고 한다. 2세대(2G)기술들인 TDMA, GSM, CDMA들은 전송속도가 9.6~14.4kbps(키로비트매초)로서 오늘의 보통모뎀속도보다 뜨다. 3G기술들은 보다 빠르고 많은 자료를 전송하게끔 설계되고 있다. 일부는 아마 고속인터네트접근뿐아니라 비데오전송도 할수 있을것으로 보인다. 아래에 3G부류에 속하는것들을 포함하여 기타 수자식전송방법을 소개한다.

- ***IDEN***(Integrateel Digital Enhanced Network : 개선된 수자식종합통신망)은 TDMA에 기초하고 있으며 2G전송방법이다. 음성과 자료를 전송하는외에 대공전화기(walkie–talkie)처럼 두대의 iDEN전화사이의 쌍방향라지오통신에도 쓰인다.
- ***PDC***(Personal Digital Communications : 개인용수자식통신)는 TDMA에 기초한것으로서 일부 나라에 널리 쓰이는 2G전송방법이다.
- ***GPRS***(General Packet Radio Service : 일반파케트라지오봉사)는 2.5G(3G는 안되고)기술로서 그 기초는 GSM이다. 이것은 파케트교환형식의 자료기술로서 《항상 직결》적인 접속상태를 유지한다. 즉 하루종일 전화망에 가입상태에 있으면서 보내거나 받을 자료가 실지 있을 때에만 가입자가 리용한다. 최고자료전송속도는 115kbps이다.
- ***EDGE***(Enhanced Data rates for Global Evolution : 세계공용자료속도개선체계)는 TDMA와 GSM에 기초한 3G기술이다. GPRS와 같이 파케트교환식자료기술로서 《항상 직결》상태를 유지한다. 최고자료속도는 384kbps로 예상한다.
- ***UMTS***(Universal Mobile Telecommunications System : 국제이동통신체계)는 GSM에 기초한 3G기술이다. 최고자료전송속도는 2Mbps로 예상된다.
- ***CDMA2000***과 ***W–CAMA***(wideband CDMA : 광대역CDMA)는 두가지 다 CDMA에 기초한 3G기술들이다. CDMA 2000은 북아메리카설계안이고 W−CDMA는 유럽과

일본식설계안들이다. 둘다 최고자료속도가 저속이동전화일 때 384kbps이고 고정전화일 때 2Mbps이다.

그 속도나 방법에는 관계없이 이동전화와 인터네트 혹은 인트라네트싸이트사이에 비밀성을 보장하자면 반드시 말단 대 말단암호화를 해야 한다. 무선인터네트통신은 무선과 유선전송을 다 포괄하기때문에 무선통신부분만을 포괄하는 암호화는 분명히 충분하지 못하다. 말단 대 말단비밀보장을 위해서는 응용프로그람들과 규약이 일정한 역할을 수행해야 하는데 이에 대해서는 후에 설명하기로 한다.

무선장치들은 어느 정도 안전한가

오늘날 기업망에서 적용되고 있는 인터네트보안은 사실 여러가지 리유로 하여 무선전화와 PDA에 응용하기 힘들다고 할수 있다. 이 기구들은 CPU, 기억기, 대역너비, 보관능력이 제한되여 있다. 결과 속도가 뜨며 계산능력이 제한되여 있다. 보통의 콤퓨터에서는 1초도 안걸리는 강력한 보안성능들이 무선기구들에서는 몇분이나 걸리므로 쓰기 불편할뿐아니라 비현실적이기도 하다. 이 기구들의 능력이 일반적인 워크스테이션하드웨어능력의 몇분의 일밖에 안되기때문에 인터네트보안의 견지에서 보면 이 무선기구들의 보안특성들은 경량형 아니면 아예 없는것이나 같다. 그러나 이 기구들을 리용하여 기업의 인트라네트기밀에 접속도 하고 있으며 이동형상거래나 은행거래도 하고 있다. 이 무선장치들이 어느 면으로 보나 작지만 그 보안상 요구는 이전과 같이 매우 중요하다. 이 무선설비들이 회사망에 널리 퍼지게 되는것과 관련하여 만일 회사의 정보기술 및 정보보안부서들이 이 무선설비들을 홀시하게 되는 경우 이것은 하나의 큰 실책이 될수 있다. 결국 이 장치들도 차별이 없다. 즉 설계를 어떻게 하는가에 따라 망의 그 어느 부분처럼 회사정보에 도청을 할수 있다. 이 장치들과 관련한 보안상 측면의 일부를 여기서 설명하자.

인증

무선전화사용자를 인증하는 과정은 지금까지 몇해동안의 실천과 발전단계를 거쳤다. 무선봉사의 도난을 막기 위하여 봉사제공자들이 여러해동안 기울인 노력을 놓고 보더라도 인증과정은 오늘날 수자식이동전화의 가장 강력한 보안특성의 하나로 될것이다. 자기들이 제공하는 전화봉사의 사용자에게 료금을 받아 내는것은 봉사사용자들이 매우 관심하는 문제이기때문에 이동전화사용자인증은 최고의 중요성을 가진다.

앞에서 언급한바와 같이 GSM전화는 사용자인증정보를 담은 SIM카드나 소편을 사용한다. SIM에는 흔히 인증 및 암호화열쇠들, 인증알고리듬, 식별정보, 사용자전화번호 등이 있다. 이것을 가지고 사용자는 자기 전화와 자기가 가입한 전화망에 대한 인증을 한다.

북아메리카에서는 TDMA와 CDMA전화들이 GSM과 같은 복잡한 인증방법을 사용한다. GSM과 마찬가지로 이 인증방법은 열쇠, 인증쎈터, 문제–대응기법 등을 혼용한다. 그

러나 TDMA와 CDMA전화들은 외장식SIM카드나 소편을 리용하지 않으므로 이 전화들은 대신 전화기에 내장된 인증정보에 의거한다. 사용자의 신원은 결국 이 하나의 전화안에 다 있는셈이다.

뚜렷한 약점이라고 볼수 있는것은 인증에서 TDMA와 CDMA전화들은 GSM전화에 비해 그 유연성이 적은것이다. GSM전화에 새 사람을 인증시키려면 많은 경우 SIM카드나 SIM소편만 갱신하면 다 된다. 그러나 TDMA와 CDMA에서는 새 사람을 인증시키려면 비용이 많이 들어도 새 전화를 사용하는수밖에 없다. 전화를 하나 사는것보다 외장소편을 갱신하는것이 더 쉬우므로 결국 GSM에서 제공되는 보안특성들과 혁신안들을 더 탐구해야 할것으로 예견된다.

그러나 여기에서 중요한 문제는 이러한 행위의 인증이 인터네트상에서의 거래에서는 잘 적용되지 않는다는것이다. 이 방법의 인증은 이동전화사용자를 봉사제공자의 전화망에 인증시키는 역할밖에 못한다. 바로 이 망은 인터네트상에서의 거래에서 한 부분에 지나지 않는것이다. 말단 대 말단인터네트거래를 안전하게 하자면 사용자는 자기가 접속하는 인터네트 Web봉사기를 인증하여 그 봉사기가 합법적인가를 확인해야 할것이다. 마찬가지로 인터네트 Web봉사기로 자기에게 접속하는 무선사용자를 인증하여 그 사용자가 합법적인가 아니면 위장한 사용자인가를 확인해야 한다. 그러나 무선봉사제공자들은 이동전화로부터 인터네트 Web봉사기까지의 완전한 말단 대 말단인증제공을 거의 하지 않고 있다. 그 책임은 흔히 안터네트 Web봉사기와 Web응용프로그람의 소유자들의 몫으로 된다.

말단사이의 인증을 제공하는 여러가지 방법들은 오늘날 응용준위에서 시험되고 있다. 안전한 이동형상거래응용프로그람들은 대체로 신원과 통과암호와 같은 낡은 식을 사용하고 있는데 이것들은 단일요소인증만을 제공하기때문에 제한성이 있다. 다른 연구기관들에서는 SIM에 공개 및 비밀열쇠쌍, 수자식인증서를 비롯한 PKI요소들과 같은 보안사항들을 추가함으로써 GSM, SIM에 대하여 실험중에 있다.

그러나 수자식인증서사용은 공정에 부하가 많이 걸리므로 이동전화와 손에 드는 형식의 기구들에는 대체로 이 보안요소들의 경량판을 쓴다. 무선기구들에 있는 작은 처리장치들에 맞게 하기 위하여 수자식인증서와 그와 관련된 공통열쇠들은 무선장치의 자원에 따라 탁상형콤퓨터 Web열람기에 설치된것들보다 더 작거나 더 약할수도 있다.

또한 일부 기관들에서는 무선장치들에서의 인증, 수자식인증서, 공통열쇠암호화에 대하여 타원곡선암호화(ECC)라는 방법도 시험중에 있다. ECC는 강력한 암호화기능이 있으면서도 다른 암호화기능처럼 계산자원을 덜 쓰기때문에 이동통신기구들에 있어서 매우 리상적인 도구로 된다. 무선기구들에 ECC를 사용하는데서 앞장 서고 있는 업체들중의 하나는 Certicom회사이다.

무선인터네트인증과 관련한 기술이 점점 더 발전해감에 따라 어느 때인가는 인차 인터네트이동통신기구들이 통표, 스마트카드, 은행의 ATM카드처럼 일식으로 된 인증장치로 될것이라는것은 명백하다. 만일 사용자들이 이 향상된 이동통신기구들을 리용하여 인터네트상 거래를 시작한다면 이 장치들을 도난 당하거나 잃지 않도록 하는것이 선차적인 요구로 나선다. 외장식SIM이나 내장식기구에 담겨 진 신원정보를 잃어 버린다는것은 그것을 가지고 다른 자가 자기처럼 위장하여 전자상업거래를 진행할수 있다는것을 의미한

다. 이동장치에서는 그 사용자가 그것의 전반적보안에서 가장 큰 역할을 한다. 인터네트 접근과 내장식공통/비밀열쇠쌍이 들어 있는 이동전화를 잃어 버린다는것은 은행의 ATM 카드와 그 카드우에 쓴 PIN을 함께 잃어 버리는것만큼 파국적이거나 그보다 더할수도 있다. 만일 이러한 기구를 잃어 버렸다면 봉사제공자에게 신속히 그 분실사실과 그 사용중지를 통고하여야 한다.

비밀성

무선장치에서의 비밀성보존에는 여러가지 흥미 있는 난점들이 제기된다. 열람기로 Web싸이트에 접근해 들어 가려고 통과암호를 칠 때 대체로 쳐넣는 통과암호는 별표모양이나 빈 자리모양으로 숨겨 져 나타나서 옆의 사람들이 본인이 쳐넣는 실지 통과암호를 화면상에서 보지 못하게 된다. 이동전화나 손에 드는 장치들에서는 통과암호를 가리우는것이 타자할 때 문제점들을 일으킬수 있다. 이동전화에서 문자입력은 수자건반으로 하는데 이 방법은 시끄럽고 지루하다. 실례로 문자 R를 입력하려면 수자 7을 세번 눌러야 정확한 문자가 입력된다. 입력결과가 가리워 지게 하면 무슨 글자가 실지 입력되였는지 사용자는 알수가 없다. 이러한 불편한 점이 있으므로 일부 이동인터네트응용에서는 이 마스크기능을 없애고 전체 통과암호가 실지 글자로 화면에 직접 현시되게 한다. 일부 응용에서는 처음에는 통과암호의 매 글자가 타자치는 몇초동안 직접 현시되였다가 다음에는 인차 매 글자가 빈칸으로 가리워 진다. 이렇게 하면 사용자는 정확한 글자가 입력되였는가를 알고저 하는데도 좋으며 그것을 인차 가리우게 할 필요성도 만족시켜 줌으로써 개인적비밀을 보장해 준다. 이 후자의 방법이 짐작컨대 두가지중에서 보다 유망한것으로 보이며 응용프로그람설계가들이 도입해야 할 방법이라고 본다.

비밀성보장에서 또하나의 문제는 통과암호나 신용카드번호 같은 극비정보들이 이동장치를 사용한 다음에는 그 기억기에서 소멸되게끔 하는 문제이다. 많은 경우 무선인터네트응용에서는 이러한 기밀정보들이 변수로 보관된 다음에는 그 장치의 기억기에 숨겨진다. 이동전화기에 남아 있던 신용카드번호를 그 전화기를 빌려 쓴 사람이 다시 리용하였다는 자료들도 있다. 다시한번 응용설계가들은 여기서 각성하여 비밀성보장에서 주인이 되여야 한다. 프로그람작성자들이 사용후 이동전화의 기억기에서 기밀정보들이 소실되게끔 응용프로그람을 설계하는것이 중요하다. 물론 이런 정보들을 기억기에 그냥 남겨두면 다음번에 그것을 다시 입력하는 품을 덜수 있지만 이렇게 하는것은 자기의 은행 ATM카드에 해당 PIN을 써놓는것과 꼭같이 위험하다.

다른 또하나의 문제는 인터네트상에서 무선장치로부터 목적지까지의 정보흐름 전 구간에 걸쳐 기밀정보의 비밀성이 보장되게 하는것이다. 전통적으로 보면 유선인터네트에서는 거의 모든 Web싸이트들이 안전소케트층(SSL)규약이나 그 후신인 통신층보안(TLS) 규약을 리용하여 의뢰기로부터 Web봉사기까지의 말단 대 말단의 전체 구간을 암호화한다. 그러나 많은 무선장치들 특히 이동전화는 SSL을 충분히 실행할만큼한 계산능력과 대역너비를 가지고 있지 못하다. SSL의 주요구성요소의 하나는 RSA공개열쇠암호화이다. 해당 Web싸이트에 적용되는 암호화강도에 따라 이 형태의 공개열쇠암호화가 처리기에 부하를 줄수도 있고 대역너비에 부하를 줄수도 있으며 그리하여 통과가 너무 느려 계속

하지 못할 정도로 그 장치를 혹사시킬수 있다.

대신 무선응용규약(WAP)을 리용하여 개발한 무선인터네트응용프로그람은 여러가지 보안규약을 종합하여 쓰고 있다. 안전한 WAP응용프로그람들은 SSL과 WTLS(무선통신층 안전규약)를 다같이 리용하여 서로 다른 마디의 안전전송을 보호한다. 표준적으로 SSL은 유선구간을 보호하며 WTLS는 주로 무선구간을 보호한다. 말단 대 말단 암호화와 맞먹는 것을 얻자면 두가지를 다 리용해야 한다.

WTLS는 동작상 SSL과 류사하다. 그러나 WTLS가 RSA나 ECC중의 하나를 지원하지만 ECC가 더 좋다. 그것은 ECC가 강한 암호화기능들이 있으면서도 RSA보다 밀집도가 더 좋으며 속도도 더 빠르기때문이다.

WTLS는 또한 SSL과 다른 차이점을 가지고 있다. WTLS는 속도가 느리고 자원에 대한 부하가 적은 환경에서 암호화를 진행하지만 SSL은 이러한 환경에는 무리를 줄수 있다. 그것은 SSL암호화에는 믿음직한 통신규약 특히 TCP(TCP/IP의 일부분인 송신조종규약)가 필요하기때문이다. TCP는 오유탐지, 통신수락통지, 재송신기능들이 있으므로 송신과 수신에서 신뢰성을 보장한다. 그러나 이 기능으로 하여 TCP는 보통 무선설비들보다 더 많은 대역너비와 자원을 소모한다. 대부분의 이동통신결선들은 오늘날 대역너비가 좁고 속도가 느리며 TCP가 만들어 내는 부단히 가고오는 오유탐지전송량을 처리하게끔 되여 있지 못하다.

이 제한성들을 인식하고 WAP의 표준화를 추진할 책임을 맡고 있는 단체인 WAP연단은 무선환경에 보다 적합한 보충적인 규약묶음을 내놓았다. 이 환경이 대개 접속속도가 낮고 신뢰도가 낮으며 대역너비도 좁기때문에 이것들을 보충하기 위하여 그 규약묶음은 압축된 2진자료대화를 리용하며 불균일한 포괄구역에 대해서 허용도가 높다. WAP규약묶음은 OSI참조모형의 4, 5, 6, 7계층들에 속한다. WAP규약묶음은 IP형망들에서는 UDP(사용자데타그램규약)와 협동하며 비IP형망에서는 WDP(무선데타그램규약)와 협동한다. WAP규약묶음에 속한 보안규약인 WTLS는 무선환경에서 UDP나 WDP전송을 보호하는데 쓰인다.

WTLS과 SSL사이의 이러한 차이 그리고 그것들의 작업환경상 차이로 하여 하나의 환경에서 다른 하나의 환경에로 이동되는 전송자료들을 변환해 주는데 관문과 같은 중간장치가 필요하다. 이 관문을 흔히 WAP관문이라고 한다. 이 WAP관문에 대해서는 하부시설부분에서 구체적으로 설명하기로 한다.

악성코드와 비루스

워크스테이션들과 봉사기들에 대한 수많은 공격들에 비해 보면 무선장치들의 보안에 대한 공격회수는 지금까지 적다. 이것은 부분적으로는 악성코드와 비루스가 교묘하게 리용할수 있는 충분한 처리기, 기억기나 보관기가 이동전화 같은 대부분의 이동통신장치들에 없다는 단순한 사실과 관련되여 있다. 실례로 오늘날 비루스를 퍼뜨리는 인기 있는 방법은 전자우편뒤의 첨가파일에 비루스를 숨기는것이다. 그러나 이동전화 같은 대부분의 이동통신장치들은 전자우편의 추가파일을 보관하거나 열어 볼 능력이 없다. 이것으로 하여 파괴적인 잠재력이 비교적 낮은 무선장치들은 공격대상으로는 상대적으로 적합하지

않다.

그러나 계산능력, 기억능력, 보관능력이 더욱더 커짐에 따라 이동통신장치들에 대한 공격가능성은 더욱 높아 질것이다. 속도가 더 높아 지고 내리적재능력이 더 빨라 지고 처리가 더 개선되면 이동통신장치들은 오늘날의 워크스테이션처럼 해커들에게 좋은 먹이감으로 될수 있을것이다. 이 장의 집필당시 이동전화제작업체들은 다음세대 이동전화들이 쟈바와 같은 언어들을 지원함으로써 사용자들은 일정계획프로그람, 계산프로그람, 유희프로그람들을 자기들의 Web용전화들에 내리적재할수 있을것이라고 이미 발표하고 있었다. 그러나 부정적인 견지에서 보면 이렇게 되면 사용자들이 자기도 모르게 악성프로그람(즉 《악성웨어》)들을 자기들의 무선통신도구들에 내리적재하게 될수 있는 가능성이 많다는것이다. 다음의 격언이 무선기구들에 꼭 맞는다. 《두뇌들이 많을수록 더 큰 목표로 되기 쉽다.》

망하부시설들은 어느 정도 안전한가

정보보안분야에서 오래동안 일해 온 사람들이 알다싶이 보안은 많은 구성요소들의 집합으로 이루어 지나 그 총체적세기는 바로 가장 약한 고리가 얼마나 센가 하는데 달려 있다. 때로는 망에서 가장 강력한 암호화기술을 쓰고 말단장치에서 가장 강력한 인증기술을 리용해도 소용없이 되는 경우도 있다. 전반적인 련쇄고리중에서 그 어느 곳이든 약한 고리가 있으며 공격자들은 이 취약점에 집중공격을 들이대여 마침내는 녹여 내고 최소의 노력에 최소의 자원이 필요한 경로를 택하게 된다.

무선인터네트세계는 아직 상대적으로 청소하고 발전도상의 분야이므로 정도의 차이는 있겠으나 취약성은 허다하다. 여기에서는 WAP(무선응용규약)를 사용하는 사람을 위하여 일부 하부시설의 취약점들을 집중적으로 보기로 한다.

WAP에 있는 빈 구석

암호화는 전자상업거래세계에서 정말 귀중한 도구로 되여 왔다. 많은 직결기업들은 SSL이나 TLS를 리용하여 전 구간의 암호화를 진행함으로써 의뢰기와 Web봉사기사이의 인터네트거래를 보호한다.

그러나 WAP를 사용할 때 대화를 위한 암호화가 설정되면 여기에는 두가지 구역의 암호화 즉 전송의 서로 다른 1/2을 보호하는 암호화가 적용되게 된다. SSL이나 TLS는 주로 Web봉사기와 이미 실행한 WAP관문이라고 하는 중요한 망장치사이의 첫 구간만 보호하게 된다. WTLS는 WAP관문과 무선이동통신장치사이의 두번째 구간을 보호한다.

이 WPA관문국은 무선전송에 부합되게 유선신호를 대역너비부하가 적고 압축된 2진수형태로 변환하는데 필요한 하부시설구성요소이다. SSL과 같은 암호화가 대화과정에 리용되면 WAP관문은 이 SSL전송자료를 복호화하였다가 다시 그것을 WTLS로 재암호화하며 반대방향인 경우에는 이 과정을 거꾸로 거침으로써 SSL에 의하여 보호되

는 전송을 변환해 주게 된다. 이 변환은 몇초밖에 걸리지 않는다. 그러나 이 짧은 과정에 그 자료는 WAP관문의 기억기에 복호화되고 평문으로 앉아 있다가 비로소 두번째 규약을 리용하여 재암호화되게 된다. 일부 사람들이 《WAP의 빈 구석》이라고 부르는 WAP관문에서의 이 짧은 공간은 해커의 공격을 받을수 있는 하나의 취약점이다. 결국 WAP관문이 어디에 위치하고 있는가, 얼마나 안전하게 관리되는가, 누가 그 보호책임을 지고 있는가에 달려 있다.

명백히 말하여 WAP관문은 안전한 환경에 위치하고 있어야 한다. 그렇지 않으면 그 관문에 접근하려는 침입자가 평문으로 되는 순간에 기밀자료들을 도적질할수 있다. 또한 침입자는 관문에서 암호화과정을 교환시킬수 있으며 지어 봉사거부공격을 유발시키거나 이 기구에 기타 악성공격도 들이댈수 있다. 비법접근으로부터 관문을 지키는것뿐아니라 그 보안상태를 향상시키기 위하여서는 또한 운영절차도 잘 지켜야 한다. 실례로 복호화와 재암호화과정이 진행될 때 평문자료를 디스크기억매체에 보관하지 않는것이 좋다. 이 자료를 사용기록파일에 보관하는것도 역시 공격자들에게 불필요하게 공격호기심을 가지게 하는것으로 될수 있다. 또한 복호화와 재암호화는 반드시 기억상에서만 진행되여야 하며 그것도 가능한껏 빨리 진행되여야 한다. 뿐만아니라 우발적인 로출을 방지하기 위하여 기억기는 정확히 덧쓰기를 진행하게 함으로써 그 어떤 기밀자료도 다 소실된 다음에야 그 기억기가 재리용될수 있게 하여야 할것이다.

WAP관문전개구조

자료의 기밀성과 그 자료의 비법적인 공개에 대한 법적책임성문제가 제기되여야 안전한 무선봉사업체(고객들도 같이)들은 WAP관문이 어디에 위치하고 있으며 어떻게 보호되고 있으며 누가 그것을 보호하고 있는가에 대하여 우려하게 된다. 세가지 가능한 전개구조와 그 보안내용에 대하여 구체적으로 보자.

봉사제공자에 위치한 WAP관문 대부분의 경우 WAP관문들은 무선봉사제공자들이 소유하고 운영한다. 안전한 무선응용체계들을 리용하고 있는 많은 기업들은 오늘날 이러한 봉사제공자들의 WAP관문에 의거하여 SSL–WTLS응용체계들을 소유한 기업들과 그 사용자들이 WAP관문과 그것을 통과하는 기밀자료들을 바로 이 무선봉사제공자들이 안전하고 사고없이 지켜주기를 알고 있다는것을 의미한다. 그림 8－1에서는 WAP관문봉사제공자들의 안전환경안에 있는 설치형태를 보여 주고 있다. 사용자의 이동전화와 기업의 방화벽뒤에 있는 응용봉사기사이의 대화에 암호화가 적용된다면 그 이동전화와 봉사제공자의 WAP관문사이의 구간에 대한 암호화는 WTLS가 해준다. WAP관문과 기업호스트의 응용봉사기사이구간의 암호화는 SSL이나 TLS를 리용하여 한다.

이러한 설치방식으로 안전한 WAP응용체계들을 전개하는 기업이 알아야 할것은 짧은 순간이나마 복호화되여 평문상태로 있다가 다시 암호화되는데 이 과정이 회사자체의 관할밖에 있는 관문에서 진행되는것이므로 자료의 말단간보안은 담보될수 없다는것이다. WAP관문은 대개 무선봉사제공업체의 자료쎈터안에 전개되여 있으며 그 기업에 직접적인 책임을 지지 않는 사람들이 관리한다. 물론 WAP관문을 안전하게 그리고 안전한 자리에 보존하는것은 봉사제공자의 최상의 리익에 부합되는 일이다.

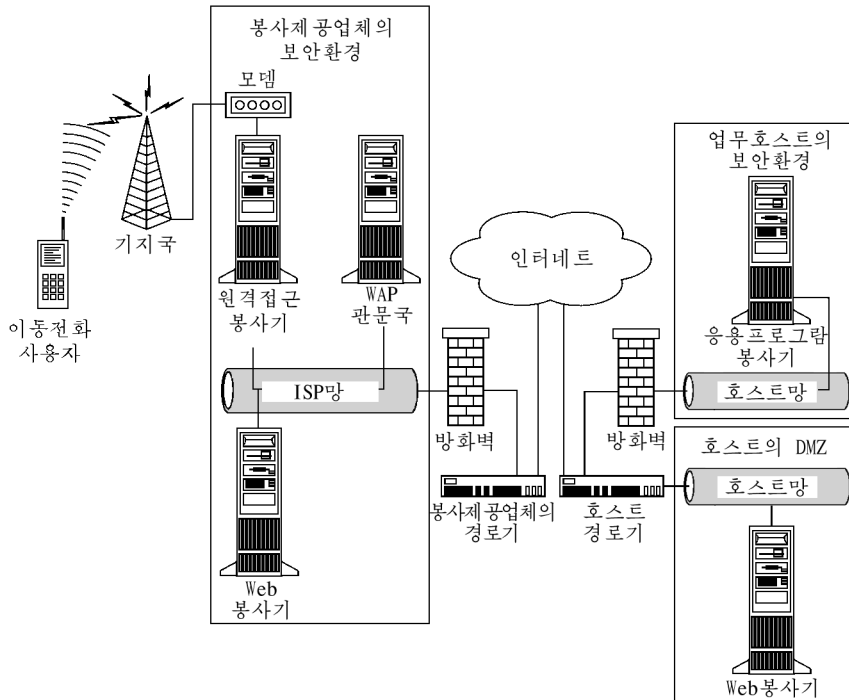



그림 8－1. 봉사제공자에게 있는 WAP관문

때로는 그 신뢰를 확인보강하기 위하여 기업들은 봉사제공자의 WAP관문운영실태에 대한 정기적인 보안검열을 진행하여 위험요소들이 최소화되게끔 할수도 있다. 그러나 기업들이 검사해야 할 WAP관문수는 봉사제공자수가 많으므로 상당한 수에 달한다. 봉사제공자나 WAP관문을 설치한 주되는 목적은 무선전화가입자들에게 인터네트접근봉사를 하려는데 있다. 가령 사용자들이 한 기업의 안전한 Web싸이트를 무선전화로 방문한다고 할 때 전 세계적으로 20개소의 무선봉사제공업체를 통해야 한다면 그 기업은 이 20개소의 봉사제공자들에 속하는 WAP관문들을 모두 검사해야 한다. 이것은 말그대로 엄청난 과제일뿐아니라 보안담보의 실천적인 방법이 못된다. 매 봉사제공자 역시 각이한 방법으로 자기들의 WAP관문을 보호할것임은 틀림없다. 더우기 대부분의 경우 무선봉사제공자들은 자기의 이동전화가입자들앞에 책임을 지지 그 어떤 계약관계가 없는 한 안전인터네트응용체계를 가지고 있다고 하여 그 무수한 기업들앞에 책임을 질 필요는 없는것이다.

호스트에 위치한 WAP관문 금융, 보건, 정부기관들을 비롯한 일부 기관들과 업체들은 자기의 고객들의 기밀자료들을 보호해야 할 법적의무를 지니고 있다. 기관의 내부통제권밖에 이러한 기밀자료들이 로출되게 되면 불필요한 위험 및 그 법적손해에 대한 책임이 제기된다. 일부 기관들에 있어서 《WAP 빈 구석》은 깨진 송유관과 비슷하여 이 비밀을 어서 가져 가 달라고 하는것과 같은 완전한 비밀성의 위반으로 된다. 이러한 현상을 극복하는데는 하나의 가능한 방도 즉 WAP관문을 기업의 호스트자체의 보호된 망에 설치

하여 무선봉사제공자의 WAP관문을 완전히 무시하는 방도가 있다. 그림 8－2에 이러한 설치방식의 례를 주었다. Nokia, Ericsson, Ariel Communications회사들은 이러한 대안을 제공하는 대표적인 판매업체이다.

이 방식을 쓰면 WAP관문과 그 WTLS–SSL변환과정이 안전한 Web응용을 제공하는 그 기관내의 신뢰성 있는 위치에서 보호되고 진행된다는 장점이 있다. 이 방식에서 사용자는 무선전화기에서 번호판을 돌려 직접 봉사제공자의 공공교환전화망(PSTN)을 거쳐 기업의 원격접근봉사기(RAS)로 들어 온다. 일단 RAS에 들어 오면 전송이 계속 이어 져 WAP관문을 거쳐 응용봉사기나 Web봉사기에 도달하는데 이 모든 기구들은 다 기업호스트자체의 안전환경내에 위치하고 있다.

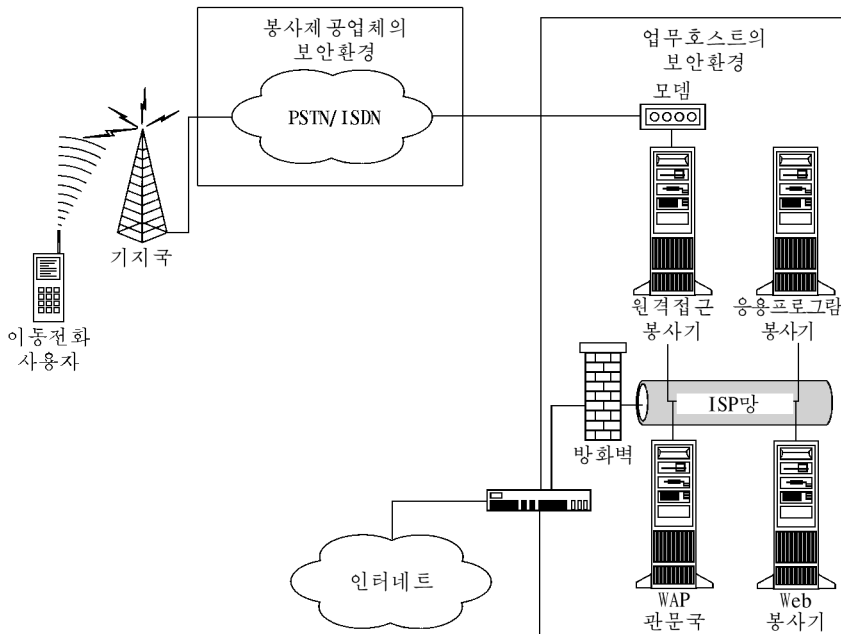



그림 8－2. 호스트에 있는 WAP관문

이 방식이 말단사이의 보안을 더 좋게 하지만 약점이 있는데 그것은 기업호스트가 사용자들이 충분한 접근점을 가지도록 수많은 모뎀들과 RAS를 설치하지 않으면 안된다는 점이다. 또한 그 기업이 봉사제공자의 WAP관문대신 자기 WAP관문에로 직접 들어 오게끔 매 사용자들의 이동전화와 PDA들을 재설정해 주지 않으면 안된다는 것이다. 그런데 모든 이동전화들이 사용자에 의한 재설정을 다 허용하는것도 아니다. 게다가 일부 이동전화들은 오직 하나의 WAP관문만 지적하게 되여 있으며 일부는 다행스럽게도 하나이상을 지적하게 되여 있다. 두 경우 다 기업자체의 WAP관문을 지적하게끔 모든 무선장치들을 개별적으로 재설정해 주는것은 품과 시간이 상당히 들수 있다.

오직 하나의 WAP관문만 지적하게 된 이동전화의 사용자들에게 있어서 이 재설정은

또 하나의 문제점이다. 이 사용자들이 인터네트상의 다른 WAP관문에 접근하려면 그 기업호스트의 WAP관문을 먼저 통과해야 한다. 만일 그 호스트가 밖으로 나가는 전송자료를 허용하면 그 호스트는 자기 WAP관문지적을 새로 설정한 이 사용자들에게 있어서 하나의 인터네트봉사제공자로 된다. 림시 ISP로 역을 해야 하는 호스트로서는 불가피하게 통신문제와 사용자관계문제까지 돌보아 주어야 하며 결국 상당한 량의 자원소모로 하여 청하지 않은 부담을 걸머지게 된다.

봉사제공자의 WAP관문으로부터 호스트WAP대리자(proxy)에로의 경유 말단사이안전암호거래는 바라지만 자체의 WAP관문을 설치해야 되는 행정적두통거리를 안고 있는 기업들에 있어서 일련의 다른 방도도 있다.

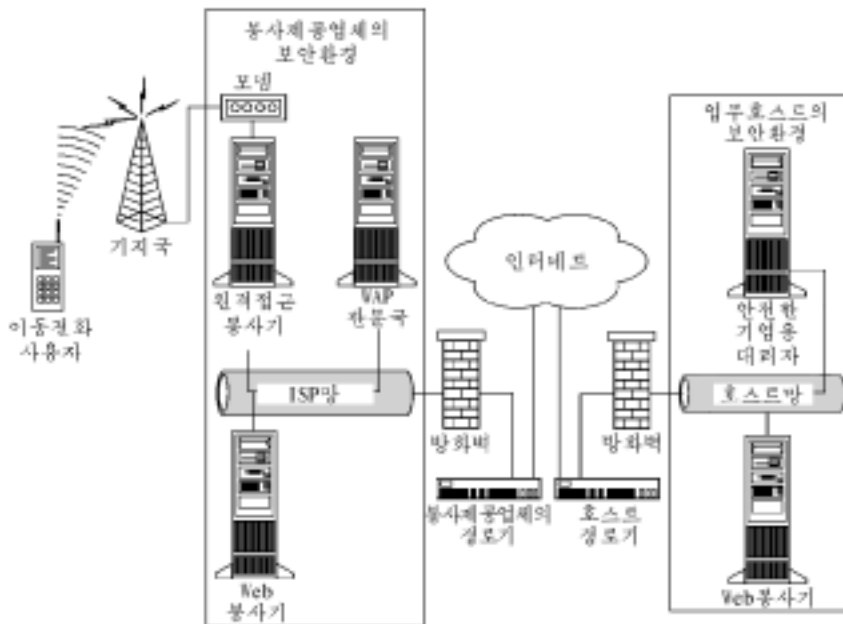



그림 8－3. 봉사제공자의 WAP관문에서부터 호스트의 WAP대리자에로의 경유

그림 8－3에서 보는바와 같이 이러한 한가지 방도로서는 WTLS로 암호화된 자료를 변환시키지 않고 사용자의 이동전화로부터 봉사제공자의 WAP관문을 경유시키는것이다. 기업호스트자체의 안전한 망내부의 두번째 WAP관문 비슷한 장치에 이 암호자료가 도달할 때까지 WTLS–SSL암호화변환은 진행되지 않는다. 이 방안을 현재 개발하고 있는 하나의 업체는 Openwave Systems(Phone.com과 Software.com의 결합체)이다. 이 업체는 이 두번째 WAP관문 비슷한 장치를 안전기업대리자라고 부른다. 암호화된 전 대화기간 봉사제공자의 WAP관문과 기업의 안전기업대리자는 서로 잘 협동하여 이 암호화된 자료를 변함이 없이 안전기업대리자에 넘겨 준다. 이 방안에서 봉사제공자의 WAP관문을 쓰게 되는 리유는 이것이 이동통신사용자들에게 정확한 인터네트접근

을 보장하면서도 WTLS–SSL암호변환은 하지 않으며 따라서 기밀자료를 루설할 가능성이 없기때문이다.

복호화작업은 기업의 안전망안에 있는 안전기업대리자나 응용봉사기에서 진행된다.

그러나 이 방법의 한가지 결함은 그것이 독점적성격을 띤다는데 있다. 이 글을 집필하는 당시에는 Openwave사의 해결책이 은을 내게 하기 위하여 세개소에서 Openwave회사의 독점적부품들을 전개해야 하였다. 무선봉사제공자는 Openwave의 최신 WAP관문을 구입하여 사용해야 하며 안전응용을 제공하는 기업은 Openwave의 안전기업체대리자를 사용해야 그 WAP관문과의 암호화경유과정을 순조롭게 해결할수 있다. 게다가 무선장치들자체도 역시 Openwave의 Web열람기, 적어도 Micro–browser 제5판을 리용해야 한다. 전세계에서 WAP를 리용하는 전화들의 70%가 Openwave의 Micro–browser판들을 리용하지만 대부분의 이 전화들은 3판이나 4판을 쓰고 있다. 그런데 이 현존 열람기들은 대부분 사용자에 의한 판본갱신이 안되게 되여 있어 모든 사용자들이 이 대안을 리용하려면 전화기들을 새로 사지 않으면 안되게 되여 있다. 이것으로 하여 이 대안이 성숙되여 대중화되려면 시간이 일정하게 걸릴것이다.

이것들은 무선인터네트장치들의 말단사이 암호화를 보장하는 유일한 방도들로는 되지 않는다. 현재 추진중에 있는 기타 방도들에는 응용준위에서의 암호화적용, 이동전화의 SIM카드에 암호화열쇠와 암호화알고리듬의 추가, WAP기술사항의 갱신에 보다 강력한 암호화기법들을 추가하여 《WAP의 빈 구석》을 완전히 메꾸는것 등도 포함되여 있다.

결 론

정보보안분야의 여러 전문가들에게 권고하려는 두가지 사항이 있다.

- 무선보안문제점들과 대안들의 추세를 놓치지 말것.
- 무선장치들을 홀시하지 말것.

정보기술과 정보보안전문가들에게는 새로 나오는 무선인터네트도구들을 개인용소도구나 기업인의 장난감 등으로 왜소하게 대하는 관점이 있다. 이들은 회사의 PC들과 봉사기들, 망들을 보호하느라고 너무나도 바쁘기때문에 그 어떤 새로운 형의 장치들이 나왔다 해도 그에 대하여 걱정할 시간조차 없다. 회사들의 보안방책에서는 대부분 이동전화와 같은 휴대형장치들에 대한 규제사항조차 없으나 일부 회사들은 이러한 장치들을 리용하여 자기의 내부전자우편을 교환하고 있는 실정이다. 여기서 일반적으로 잘못 생각하고 있는것은 《이 장치들이 너무나도 작은데 이 작은 장치들이 무슨 해를 끼치겠는가.》 하

는것이다.

보안부서들은 지금까지 대형콤퓨터로부터 분산되여 있는 PC들로 정보자산이 흘러 가는것과 씨름질해야 하였다. 보안의 초점을 어디에 맞추어야 하겠는가에 대하여 회사들의 관점은 대체로 일정한 정도로 개변되여야 하였다. 과장이 없이 말하여 회사의 콤퓨터사용환경은 또하나의 중요한 이행과정을 겪고 있다. 회사의 정보자산이 무선장치에 의해 접근되고 있다는것은 몇년동안 무선노트형콤퓨터가 무선접근을 하여 왔기때문인것이라기보다 그 접근도구가 점점 값이 눅으며 따라서 그 대수가 굉장히 늘어날수 있기때문이다. 3,000$짜리 노트형콤퓨터를 사용하지 않고 이제는 사용자(혹은 침입자)가 40$짜리 인터네트통신이 가능한 이동전화 한대를 가지고 어느 곳에서든지 기밀적인 회사망에 간단히 쳐들어 올수 있게 되였다. 앞으로도 이 이동통신장치들의 처리능력, 기억용량, 대역너비, 보관, 사용상 편의가 계속 개선될것이며 결국에는 대중성이 상당히 증가할것이다. 바로 이 마지막항목을 실현하는데 회사의 자원이 불가피하게 소모될것이다.

이 장치들은 작지만 기관의 기밀자료들에 접근하기만 하면 콤퓨터만큼 일을 잘할수 있고 손해도 끼칠수 있다. 정보보안적안목에서 이 장치들을 무시하거나 쓰지 못하게 하면 두가지 결과가 초래될수 있다. 첫째로, 기관내의 영업단위들이나 간부들이 무선장치와 무선봉사를 추진시켜 대개 성공적으로 도입은 하면서도 정보보안부서의 개입이나 지도를 완전히 차단해 치울수 있다. 이렇게 되면 불피코 정보보안부서들은 썩 후에야 알게 되지만 정확한 설계와 계획을 하게끔 도와 주기에는 너무나도 때 늦은것이다.

둘째로, 무선장치들과 그 능력들에 대하여 무시해 버리는 경우 정보보안부서는 누구도 돌보지 않고 무방비상태로 된 창문을 공격자들에게 열어 줄수 있다. 이러한 기관들은 무선장치를 사용한 공격만 있으면 꼼짝 못하고 녹아 나게 된다.

무선장치들을 단순한 소기구들이나 시끄러운것으로 여기지 말아야 한다. 이 장치들은 일단 기관의 귀중한 정보자산으로 침투해 들어 가면 무차별적이며 망의 그 어느 마디와도 꼭 같은 역할을 한다. 추세에 민감하고 준비 있는 전문가로 되자면 정보보안실천가들은 무선기술과 관련한 보도자료들과 보안문제점들을 다 알고 있어야 한다. 또한 응용프로그람작성자들과 련합하여 사업함으로써 이 장에서 언급된 많은 문제점들을 무선응용설계에 포함시키도록 하여야 할것이다. 그리고 최종적으로는 각 기관들에서 정보보안방책에 의해 보호되고 있는 장치들의 부류를 확장하여 무선장치들까지 포함할수 있게 해야 한다. 그것은 효과상 이 무선장치들이 기관의 하부시설의 또하나의 구성요소로 되기때문이다.

참 고 문 헌

도 서

1. Blake, Roy, *Wireless Communication Technology*, Delmar Thomson Learning, 2001.
2. Harte, Lawrence et al., *Cellular and PCS: The Big Picture*, McGraw-Hill, 1997.
3. Howell, Ric et al., *Professional WAP*, Wrox Press Ltd., 2000.
4. Muller, Nathan J., *Desktop Encyclopedia of Telecommunications, second edition*, McGraw-Hill, 2000.
5. Tulloch, Mitch, *Microsoft Encyclopedia of Networking*, Microsoft Press, 2000.
6. Van der Heijden, Marcel and Taylor, Marcus, *Understanding WAP: Wireless Applications, Devices, and Services*, Artech House Publishers, 2000.

기사와 소론문

1. Saarinen Markku-Juhani, *Attacks Against the WAP WTLS Protocol*, University of Jvyskyl, Finland.
2. Saita, Anne, Case Study: Securing Thin Air, Academia Seeks Better Security Solutions for Handheld Wireless Devices, http://www.infosecuritymag.com, April 2001.
3. Complete WAP Security from Certicom, http://www.certicom.com.
4. Radding, Alan, Crossing the Wireless Security Gap, http://www.computerworld.com, Jan. 1, 2001.
5. Does Java Solve Worldwide WAP Wait?, http://www.unstrung.com, April 9, 2001.
6. DeJesus, Edmund X., "Locking Down the... Wireless Devices Are Flooding the Airwaves with Millions of Bits of Information. Securing Those Transmissions Is the Next Challenge Facing E-Commerce, http://www.infosecuritymag.com, Oct. 2000.
7. Izarek, Stephanie, Next-Gen Cell Phones Could Be Targets for Viruses, http://www.fox-news.com, June 1, 2000.
8. Nobel, Carmen, Phone.com Plugs WAP Security Hole, *eWEEK*, September 25, 2000.
9. Secure Corporate WAP Services: Nokia Activ Server, http://www.nokia.com.
10. Schwartz, Ephraim, Two-Zone Wireless Security System Creates a Big Hole in Your Communications, http://www.infoworld.com, Nov. 6, 2000.
11. Appleby, Timothy P., WAP — The Wireless Application Protocol (White Paper), Global Integrity.
12. Wireless Devices Present New Security Challenges — Growth in Wireless Internet Access Means Handhelds Will Be Targets of More Attacks, CMP Media, Inc., Oct 21, 2000.

제9장. 가상개별망배비와 평가전략

케이스 파슬리

최근년간 가상개별망(VPN)기술은 그 성능과 사용상 편리, 설치, 관리도구효과성 등의 분야에서 급속히 발전하였다. VPN기술에 대한 시장의 요구도 급속히 높아 가고 있다. 이와 함께 여러가지 VPN관련제품들의 수가 늘어 나고 있다. 원가절약이라는 약속이 빈말로 되지 않고 실지 현실화되고 있다. 그러나 기술적 및 상업적견지에서 볼 때 VPN에 대한 새로운 희망이 있다. 오늘 빠른 속도로 발전하고 있는 기업환경에서 관리, 설치, 규모조절이 매우 쉬운 VPN체계를 담보하는것은 정확한 VPN체계를 선택하고 실행하는 문제가 제기될 때 매우 중요한 성공의 요인으로 된다. 기업적인 견지에서 현실적인 리익으로 되는 점은 다음과 같다.

- 영업동반자나 고객들과의 보다 밀접한 련계로 인한 경쟁력향상
- 봉사제공의 새로운 통로
- 적은 원가로 새로운 시장진출
- 지난 시기 골치거리로 되였던 보안상 우려를 해소하고 보다 높은 가치의 정보를 제공하는것

선택할것이 많은 조건에서 최적의것을 어떻게 결정하겠는가. 객관적인 기준이 있어 판매업체의 상품소개내용을 공정하게 평가할 필요가 있다. 업체의 성능소개에 대한 평가를 할 때 무엇을 중시해야 하겠는가. VPN체계에서 그밖에 또 리익으로 되는 점은 무엇인가. 일부 경우에 보안관리봉사제공자에게 자문을 위탁해 보는것도 하나의 대안이 될수 있다. 보안관리봉사제공자란 표준적으로 보안응용프로그람들을 가지고 그것을 거래식으로 리용하면서 보안관리를 봉사해 주는 외부의 자원제공자(outsourcer)를 말한다. 많은 기업들은 VPN의 설치관리를 맡아 해주는 보안관리봉사제공자들에게 VPN을 위탁하는것을 고려중에 있다. 그것은 자체의 기술인원들보다 대형VPN을 더잘 운영해 나갈수 있는 전문인력과 관리구조를 바로 이 보안관리봉사제공자들이 가지고 있기때문이다.

VPN의 성능은 새로운 VPN제품판본들이 나옴에 따라 계속 질이 개선되고 있다. 성능이 높은것이기는 하지만 VPN선택에서 그것이 가장 중요한 기준이겠는가. 그렇지 않다. 속도는 빠르지만 침입 당하기 쉬운 VPN의 도입은 보안상 리로운 점이 없을것이다. 성능역시 판정하기 어려우며 많은 경우 성능시험은 제대로 잘되지 않으며 한갖 현실세계의 환경을 흉내낸데 지나지 않는다. 판매업체들의 성능광고도 매우 구체적으로 재판정해 보아야 한다. 그것은 시장실현위주의 관점에서 성능을 지나치게 과장하여 광고함으로써 현실에서는 제대로 성능이 나오지 않기때문이다. 판매업체들이 어떤 시험방법을 이러한 성능광고의 기초로 써먹는가를 아는것이 중요하다.

이 장에서는 VPN과 그 관련제품 선택과 도입에서 정보보안전문가들이 부닥치는 여

러가지 문제들에 대답을 주려고 한다.

VPN이란 무엇인가

VPN은 사적인 정보가 인터네트와 같은 공공망을 통하여 다른 곳에 전송되게 하는 망을 말한다. 하나의 VPN은 망체계밖의 확장부분이며 따라서 VPN에 속한 모든 입구점들에서 망보안방책을 통일적으로 실현할수 있는 능력을 가져야 한다. 교갑화와 암호화를 통하여 자료가 공공망으로 전송될 때 그 비밀성은 담보된다. 이 기술을 적절히 리용하여 얻을수 있는 기술적인 리익은 기업운영원가의 절약, 망접근보안의 개선, 중계시 자료의 무결성, 사용자 및 자료인증과 자료의 비밀성보장이다. 그러나 일부 재정적인 리익이 있다 해도 VPN구매후에 생기는 VPN체계의 실지비용 즉 배비, 관리, 지원 등에 드는 비용으로 하여 총체적으로는 재정적리익이 얼마 없다. 판매업체는 관리성, 배비성, 규모조절성의 향상에 대한 약속을 제시함으로써 자기의 제품들과 경쟁자들의 제품을 뚜렷이 구별되게 할수 있다. 이러한 형식의 제품구별화전략이 더욱 중요한것은 대부분의 업체들이 제작하는 VPN제품들이 동일한 VPN규약인 IPSec와 기타 보안기술을 리용하기때문이다. IPSec는 하나의 국제규격으로서 인터네트규약에 대한 보안적보충안들을 규제하고 있다. VPN의 실현에 쓰이는 다른 안전한 턴넬화(tunneling)규약도 있지만 IPSec는 모든 규약들가운데서 주도적인 위치를 차지해 왔다. 이 규격은 최소수준의 판매자 운용호환성에 대처하는 의무조항을 포함하고 있다. 정보보안전문가들은 이 장의 도움을 받아 IPSec VPN대안을 평가할 때 리용할수 있는 한조의 기준을 찾아 낼수 있을것이다. 설명은 VPN응용프로그람을 고찰하는것으로부터 시작된다.

IPSec VPN응용프로그람

기업들이 가상개별망(VPN)을 호기심나서 바라보게 된것은 그것이 네가지 응용적요구 즉 완전접근, 싸이트별 인트라네트, 안전한 엑스트라네트, 안전한 내부망을 만족시키기때문이다. 대부분의 경우 기술적촉매에서의 목적은 합법적인 사용자들에게 접근조종을 제공함으로써 망자료자원(봉사기파일, 디스크공유 등)을 보호하는것이다. 또한 기업적측면에서의 목적은 망하부구조의 원가를 낮추고 내부 및 외부 기업정보흐름을 원활히 높임으로써 사용자의 생산성과 경쟁력을 높이며 기업동반자들과의 관계의 강화를 보장하는것이다.

VPN평가계획에서 나서는 과업들을 명시하는것은 좋은 생각이다. 과제표를 잘 만들면 평가가 초점 있게 될수 있으며 평가완결에 필요한 자원들을 예견할수 있을것이다. 표 9－1에는 VPN평가계획과제가 례로 제시되였다.

표 9-1　　　　　VPN평가계획과제

- 자료보안요구사항을 설정한다.
- 사용자를 분류한다.
- 사용자위치를 설정한다.
- 망련결상태와 접근요구사항을 결정한다.
- 제품 및 봉사제공자를 선정한다.
- 어떤 하드웨어/쏘프트웨어를 구입할것인가를 결정한다.
- 시험운영실을 설치한다.
- 평가장치들을 구입한다.
- 특성요구사항에 기초하여 제품검수를 진행한다.
- 시험프로그람을 실행한다.

원격접근VPN

원격접근VPN에는 두가지 부분 즉 봉사기와 의뢰기가 있다. 그것들은 서로 다른 두가지 목표가 있으므로 그 평가기준도 달라야 한다.

- **기업적목표** 원거리통신비의 저하, 종업원생산능률의 증가
- **기술적목표** 원격근무자(remote worker)에게 국부망에서와 꼭 같은 안전한 접근을 제공하는것

이 장에서는 역할과 기준의 두 측면에 대하여 다 보게 된다.

원격접근IPSec VPN은 사용자들이 어느 때나 어느 곳에서나 어느것을 요구해도 기업공동의 자원에 접근할수 있게 한다.

원격접근VPN은 상사기술, 전화기술, 수자식종합통신망(ISDN)기술, 수자식가입자회선(DSL), 이동통신IP기술, 케블인터네트접근기술들을 IPSec와 같은 보안규약들과 함께 리용하여 이동전화사용자들과 원격근무자(telecommuter)들에게 안전한 접속을 보장해 준다.

의뢰기쏘프트웨어 원격접근사용자들에는 원격근무자, 이동근무자(mobile worker), 려행근무자 등 먼 거리에서 자기 회사의 자료에 접속하는 사람들이 속한다. 가장 많이 사용하는 조작체계로는 현재 회사탁상형콤퓨터표준으로 흔히 쓰는 Microsoft Windows이다. IPSec VPN의 체계요구상 Macintosh, Unix, Palm OS 혹은 Microsoft Pocket PC/Windows CE도 지원될수 있다. 더 좋기는 IPSec VPN판매업체가 회사가 요구하는 의뢰기형태들을 적당히 배합하여 제공해 줄수도 있다. 이동근무자들은 때로 판매예보, 비밀적인 환자정보나 법적정보, 고객명단, 기밀적이지만 비밀분류가 아직 되지 않은 국방성정보나 사법관계정보 등 가치가 크고 위험도가 높은 기관자료들에 접근해야 할 필요가 있다. 원격접근은 또한 동등위치접근을 하여 인터네트(레하면 Microsoft NetMeeting)상으로 정보협력한다는

것을 의미하며 원격기술지원도 가능하다는것을 의미한다.

이것을 응용하기 위한 의뢰기하드웨어의 가동환경들에는 PDA(개인휴대형정보처리기), 무릎형콤퓨터, 가정용탁상형콤퓨터, 휴대형호출기, 자료처리이동전화와 기타 유선 및 무선망설비들이 있다.

하드웨어가동환경기술이 발전함에 따라 회사자료를 원격접근할수 있는 기타 제품들이 계속 나올것이다. 인기를 끌며 계속 사용자수가 늘어 나고 있는것은 PDA, 이동전화와 같은 무선기구들과 원격접근IPSec VPN응용접근가동환경과 같은 휴대성이 높은 망관련장치들이다. 무선기구들에서 제기되는 문제들은 유선IPSec VPN 가동환경들에서 제기되는 문제들과 꼭 같은데 그런것들로는 물리적보안, 자료보안뿐아니라 계산이 힘든 기구들에서의 암호화설명을 들수 있다.

PDA와 같은 무선 IPSec VPN에서 제기되는 또 하나의 문제는 《유선세계》의 보안규약과의 호환성이다. 《무선응용규약(WAP)연단》이라고 부르는 무선규약표준화기구는 WAP에 의하여 규정된 보안규약인 《무선전송층보안》(WTLS)과 SSL과 같은 유선계통의 보안규약사이의 호환성을 개선하기 위하여 노력하고 있다. 업계의 관측자들은 PDA나 자료처리이동전화와 같은 무선기구들은 원격호상자료접근을 요구하는 응용분야에서 가장 인기 있는 가동환경으로 될것이라고 예측하고 있다. 그러나 이 기구들은 작아서 쉽게 도난 당하거나 잃어 버릴수 있다. 바로 이것으로 하여 하드웨어가동환경의 물리적보안을 IPSec VPN의뢰기쏘프트웨어의 특징분석에서 그 평가기준의 하나로 보아야 하는것이다. 이 가동환경들을 위한 물리적보안통제수단으로는 케블, 자물쇠, 계렬번호추적, 움직임수감기, 위치측정식추적(지구위치측정체계인 GPS를 리용하여), 지문스캔과 결합된 음성확인과 같은 생체계측식인증을 들수 있다.

원격접근을 위한 통신은 전화를 중심으로 계속 발전하는것이 주되는 추세로 되고 있다. 무선광대역접근방식의 사용도 계속 늘어 나는 추세를 보이고 있다. 그러나 광대역방식의 실현에서 초기에 나타났던 복잡한 문제들과 일련의 지리적제한성들이 최근년간 상당히 해결되였으므로 전화회선리용보다 광대역무선리용이 더 증가할것으로 보인다.

광대역(DSL, 케블모뎀)사용에서 나서는 한가지 문제는 봉사도 상품이므로 광대역제공업체들이 자기의 망봉사를 마디화하려고 하는것이다. 인터네트접근을 위한 케블봉사에서 나타나는 한가지 전술은 가정에 있는 사용자들이 IPSec VPN을 리용하지 못하게 하는것이다. 북아메리카의 서부해안에 있는 한 케블봉사회사에 의하면 거주형IPSec VPN사용자들로 하여 생기는 망부하때문에 대역너비가 영향을 받는다는것이다. 그리하여 이 케블봉사회사는 가정형고객들에 의한 모든 VPN사용을 금지시키고 케블모뎀에 있는 규약파케트려과규칙과 포구를 사용하게 하였다. 이것으로 회사는 분명 리익을 보는데 그것은 가정형고객들의 통신을 VPN경로조정하여 인터네트에 련결시켜 줌으로써 그들에게서 더 높은 기업준위에서의 사용료를 받아 내기때문이다. 일부 회사들은 이에 대응하여 전매특허 VPN을 내놓았는데 여기서는 VPN유효부하량을 허용된 규약(례하면 HTTP파케트)에 교갑화하여 이 케블봉사회사의 제한조치를 우회하게 하였다. 이 문제가 어떻게 해결되여 나가겠는지는 아직도 두고 보아야 하겠지만 VPN형식을 선택할 때 다른 하나의 기준도 고려해야 한다는것을 알수 있다. 즉 이 VPN형식이 말단사용자의 인터네트봉사제공자(ISP) 혹은 망접근제공자의 망에서 잘되겠는가, 원격말단사용자들이 자기 지역준위의 ISP를 사

용하겠는지, 아니면 회사가 기업준위의 접근을 구매하여 지속적이며 신뢰성 있는 련결을 보장해 주겠는지를 고려해 보아야 한다.

말단사용자들이 관심하는것은 자기들이 해야 할 일을 하고 그 보수를 받는것뿐이다. 대체로 사용자들은 자기들의 원격접근련계의 보안에 대해서는 별로 관심하지 않는다. 사용자들이 일상적으로 관심하는것은 사용상 편리, 신뢰도, 자기콤퓨터의 현존응용프로그람들과의 호환성 등이다.

따라서 전반적인 평가전략을 위해서는 VPN의뢰기를 실지생활에서 사용자가 쓰는것과 꼭 같은 원격가동환경설정값을 가지고 완전가동시험을 해보는것도 필요하다. 실례로 일부 판매업체의 개인용방화벽이 다른 업체의 IPSec VPN의뢰기와 충돌할수도 있다. 이런 비호환성은 판매업체와 련계를 맺으면 해결될수도 있고 해결 안될수도 있으나 이렇게 되면 해당 해결책에서 제외되게 된다. IPSec VPN의뢰기비호환성의 다른 실례는 한 업체의 IPSec VPN의뢰기가 IPSec VPN봉사기나 다른 IPSec VPN의뢰기의 동일한 파라메터들을 지원하지 않는데서도 볼수 있다. 여기서 잊지 말아야 할것은 표준은 흔히 최소수준의 의무적특성들만 규제해 준다는것이다. 자기 회사의 제품을 다른것들과 구별할 목적으로 업체들은 보다 발전된 특징이나 기능 즉 표준화되지 않은 특성들을 추가하는것이다. 또한 업체들은 자기 IPSec VPN봉사기와 가장 잘 호응되게끔 자기의 IPSec VPN의뢰기를 최량화할수도 있는것이다. 이런 리유로 하여 전반적IPSec VPN체계의 성능과 보안수준을 낮출수 있는 공통적인 설정의 사용이라는 업체혼용방식이 있게 된다. 실례를 들어 보면 일부 IPSec VPN봉사기판매업체들은 표준화가 명백히 되지도 않은 인증규약을 지원하고 있다. 명백하건대 선택된 IPSec VPN의뢰기가 동일한 IPSec VPN봉사기 제공업체에서 만든것이 아니여서 운용호환성이 잘되지 않으면 기준상 타협을 하든지 아니면 그 업체를 포기해야 할것이다.

인터네트가 더욱더 널리 퍼지고 가입자들이 더 오래 혹은 항상 련결상태로 있기때문에 원격 VPN사용자들의 콤퓨터가 공격을 받을수 있는 기회는 더 많이 조성된다. 따라서 원격사용자의 콤퓨터에 귀중한 자료가 보관되여 있다면 일정한 형태의 파일암호화나 디스크암호화해 놓는것이 좋다. 암호화는 처리소자에 부하를 많이 주는 과정이므로 그 콤퓨터의 계산자원이 증가하는것은 필수적이다. 여기에서 목적은 자료들을 휴대형콤퓨터에 가지고 다니더라도 결국 귀중한 그 자료들을 남이 제마음대로 훔쳐 보지 못하게 하자는것이다. 일부 VPN의뢰기용쏘프트웨어에는 비루스방지프로그람, 분산형탁상형콤퓨터용방화벽프로그람, 탁상형콤퓨터침입방지프로그람, 파일/디스크암호화프로그람이 있다. 이런것들은 일부 경우 필요이상의것으로도 될수 있지만 탁상형콤퓨터급에서도 보안이 얼마나 심화되여야 하는가를 보여 준다. 여기에 강력인증체계와 수자식서명체계를 도입한다면 보안위험은 감소된다. 앞에서 언급한것들은 전화회선사용자들에게도 적용된다. 즉 어느때든 전화회선을 통하여 콤퓨터에 련결하면 공개접근이 가능하며 따라서 공격할수 있는 IP주소를 받게 된다.

VPN의뢰기의 무결성문제도 고려되여야 한다. 실례로 VPN의뢰기가 VPN봉사기에서의 보안방책갱신 혹은 보안설정갱신을 인증할수 있는 능력이 있는지, 사용자가 일정하게 조절협력해야 갱신이 성과적으로 수행되는지 잘 알수는 없다. VPN의뢰기보안관계갱신작업과 관련하여 보면 사용자가 약한 고리로 될수 있다. 사용자의 참가가 없이 VPN의뢰기

설정을 안전하게 자동적으로 해주는 VPN의뢰기를 고려해 보는것이 좋다. 항비루스체계도 응당 있어야 한다. 그것은 트로이목마나 비루스가 VPN체계를 비법적으로 조작해 놓을수 있는 가능성이 있기때문이다. VPN의뢰기가 탁상형콤퓨터용항비루스프로그람과 호환되는지(혹은 가지고 있는지)도 알아 보아야 한다. 지난 시기에는 해커들이 목적없이 돌아 다니며 취약한 곳을 찾아 다녔다면 최근에는 특정한 목적을 가지고 겨냥한 대상에 대하여 공격하는 비률이 크게 늘어 나고 있다. 이러한 공격형태로는 VPN입구점들을 통하여 서로 조정하고 공격하는것이다. 이렇게 되면 결심을 품은 공격자는 중앙싸이트에 접속한 원격VPN사용자들을 체계적으로 녹여 낼수 있게 된다. 따라서 분산형탁상형콤퓨터용방화벽과 탁상형콤퓨터용침입탐지체계를 사용함으로써 VPN의뢰기를 보호할수 있는 요구도 제기할 필요가 있다.

분산형탁상형콤퓨터방화벽의 주요특징은 기관내의 모든 탁상형콤퓨터들에 대한 방화벽방책을 중앙조종으로 관리할수 있다는것이다. 개인용방화벽은 그 이름이 보여 주듯이 개별적인 소비자들에게 판매되는 방화벽이다. 개인용방화벽의 방책유지는 사용자가 책임진다. 분산형방화벽은 원격VPN사용자접속을 비롯한 내부망의 모든 입구점들에서 일관한 망보안방책을 중앙적으로 실시할 필요가 있는 기업들에 판매된다. IPSec VPN의뢰기와 중앙관리조종판에 보고를 제출하는 침입탐지체계를 함께 전개하면 계속되던 망공격이나 침입이 현저히 해소되고 호상 련결되여 기업의 보안상태를 잘 알수 있을것이다.

리상적으로는 IPSec VPN의뢰기와 함께 항비루스체계, 탁상형콤퓨터용침입탐지체계, 분산형방화벽 등을 같이 판매업체들에서 구입하면 좋을것이다. 그런 정도의 집적도나 종합도를 가진 제품이면 탁상형콤퓨터의 보안방책관리의 효률성을 상당히 높일수 있다.

의뢰기전개 원격접근 VPN의뢰기쏘프트웨어를 전개하는 문제들은 주로 운영적인 문제로서 SQL의뢰기쏘프트웨어와 같은 분산형쏘프트웨어에서 제기된다. 원격접근 VPN의뢰기쏘프트웨어를 전개하는데 필요한 쏘프트웨어관리지식과 방법론들은 허다하다.

VPN의뢰기의 전개성을 검토할 때 여러가지 문제점들을 고려하여야 한다. 그중 하나는 VPN의뢰기쏘프트웨어의 파일크기이다. 현재 가장 광범히 사용되는 먼거리접근방식인 저속전화회선망을 통하여 의뢰기쏘프트웨어가 배포된다면 이것은 중요한 문제로 된다. 만약 배포용FTP봉사기 같은데서 파일내리적재가 너무 시간이 걸린다면 사용자들은 시끄러워서 그 파일이나 그후 갱신판을 내리적재하지 않을것이다. 싫증을 느낀 사용자들이 있으면 VPN의 실현이 지연될것이며 결국 총적인 VPN실현원가가 높아 질것이다. 이 문제를 풀수 있는 전개전략의 하나는 VPN의뢰기를 초기에 디스케트나 CD–ROM과 같은 이동성매체에 담아 배포하는것이다. 자료압축기술을 쓰면 배포판의 크기는 상당히 줄어들것이다. 대부분의 판매업체들은 관리자가 일부 초기설정을 미리 할수 있는 일종의 의뢰기설정편의프로그람들을 먼저 배포한 다음 매 원격사용자들에게 설치파일을 배포한다. 가능한 VPN의뢰기배포방법으로는 Web싸이트나 FTP싸이트에 우편을 보내는것도 있을수 있다. Web싸이트, FTP싸이트 혹은 다른 직결파일전송방법을 리용할 때 VPN의뢰기설치파일에 비법접근할수 있는 경우도 있다는것을 정보보안전문가들은 고려해야 한다. 일부 회사들은 설치파일들을 직접 대인판매할수 있다. 우편 및 전자우편을 통한 배포의 위험을 대범하게 받아 들일수도 있다. 또 일부는 개인식별번호(PIN)나 특별한 통과암호구(passphrase)를 통하여 접근을 허용하는 안전한 파일전송싸이트를 개설할수도 있다. VPN

의뢰기의 초기배포에 대하여 말하면 배포가능성은 손해를 얼마나 보는가에 따라 허용되는 위험한도만큼 제한되게 된다. 특히 초기VPN의뢰기가 미리 설정되여 있어 그 정보를 공격자가 정탐정보로 써먹을수 있게 되는 경우에 더욱 그러하다.

의뢰기관리문제 의뢰기관리란 의뢰기설정, VPN의뢰기방책갱신과정, VPN의뢰기쏘프트웨어판본갱신 등에 대한 운영적인 유지보수과정을 말한다. 여기에도 기성지식과 기성쏘프트웨어관리방법과는 다른 문제들이 있어서 오늘 회사들이 전개한 다른 형태의 쏘프트웨어들을 관리하는데 필요할것이다. 보충적인 요인은 다름아닌 갱신판에 대한 사용자인증, VPN리용성, 갱신본파일의 무결성, 비밀성들이다. 사용자의 신임장관리능력은 VPN봉사기관리문제에 대한 부분에서 보기로 한다.

VPN의뢰기가 다른 하나의 내부망접근점이므로 이 접근은 엄격한 사용자인증과 통제가 심한 VPN설정정보를 필요로 한다. 많은 사람들은 가장 실용적인 수준의 강력한 인증은 생체계측지표에 기초한것이라고 주장할것이다. 생체계측지표들과 병행하여 PIN을 쓰면 이중인증으로 볼수 있다. 많은 보안전문가들이 다음으로 좋아 하는 방법은 스마트카드에 내장된 수자식인증서와 PIN을 결합하는것이다. 시간형계산카드(통표)와 단순통과암호들은 이제 와서는 낡은 방법으로 되고 있다. 그러나 많은 IPSec판매업체들은 IKE/IPSec(인터네트표준암호 열쇠교환규약/인터네트규약보안)표준에 XAUTH라는 보충규약을 실행하고 있다. XAUTH에서는 IPSec턴넬을 설치할 때 사용자신원확인이 필요하면 현재 가장 많이 쓰이는 인증방법인 RADIUS와 같은 기성사용자인증방법을 리용할수 있다. 보충적인 리익은 XAUTH를 리용하면 회사가 현존 인증기반체계를 리용할수 있으므로 낡은 기술에 투자를 계속 할수 있다는것이다. 결국 망의 변화가 적고 현존 사용자기록부를 다시 리용하기때문에 실행시간과 실행비용이 적어 질수 있다는것이다. XAUTH의 사용에서 약점은 통과암호와 통표사용의 취약성이 커짐으로 하여 상대적으로 인증이 약하다는것이다.

VPN갱신판봉사기를 위장할수 있는 가능성이 있는것으로 하여《의뢰기쏘프트웨어가 자기가 설정갱신판파일을 받았다는것을 어떻게 봉사기에게 확인을 보내는가?》라는 심중한 물음이 제기된다. 수많은 형태의 설정배포판이 있음으로 하여 공격자 즉 해커가 사용자들에게 비법적으로 갱신판본을 보낼수 있는 가능성이 많다. 이 위협에 대처하는 하나의 방안은 암호화기술을 리용하고 갱신판파일에 수자식서명을 하여 VPN의뢰기에 의한 확인을 한후에야 접수하는 방식이다. 보충적인 보호방법은 원격사용자콤퓨터에 실지 설정파일이 상주하고 있으므로 이 설정파일을 암호화해 두는것이다. 흔히 쓰는 하나의 수법은 갱신판본전송을 위하여 안전한 경로, 례하면 SSL보다는 LDAP를 택하는것이다.

표 9−2에는 원격접근 VPN의뢰기쏘프트웨어에 대한 평가항목의 례가 제시되여 있다. 이것들은 VPN의뢰기평가기준을 작성할 때 고려해야 할 항목들이다.

원격접근봉사기 암호화턴넬전송흐름의 주요처리는 VPN봉사기에서 진행된다. VPN봉사기는 하나의 턴넬종합점으로 된다. 즉 원격접근의뢰기는 그 봉사기를 턴넬말단점으로 리용한다. VPN봉사기가 VPN전송량을 효과적으로 처리하는 능력이 있는가 하는것을 알아 보는 방법에는 두가지가 있다. 첫번째는 더 크고 빠른 하드웨어장치를 리용하여 처리의 제한점을 극복해 보는것이다. 일체식하드웨어를 대안으로 삼으려면 하드웨어의 성능개선이 있어야 한다. 성능향상이 늦어 지면 범위확대능력이 올라 갈것이다. 이것은 흔히

표 9-2　　　　　　　　　　원격접근VPN의뢰기평가기준

전제 : VPN의뢰기가 중앙싸이트의 관리하에 있다는것을 전제로 한다.

- 이동전화사용자의 탁상형콤퓨터의 안전을 위하여 파일/디스크암호화가 필요할수 있다.
- 파일/디스크암호화를 광범하게 리용하게 되면 고성능무릎형콤퓨터나 노트형콤퓨터가 필요할수 있다.
- VPN중앙관리자에게 련결된 경보신호장치가 있는 탁상형콤퓨터용침입탐지체계
- VPN중앙관리자에게 련결된 경보신호장치가 있는 분산형탁상형콤퓨터용방화벽
- VPN의뢰기설정잠금능력
- 사용자에게 투명한 VPN의뢰기갱신
- 암호화된 링크를 통한 인증된 VPN의뢰기갱신판본
- 운용호환성이 필요한 경우 최신업계VPN표준을 철저히 지키는것

수직확대성(vertical scalability)이라고 한다. 둘째 대안은 VPN봉사기관리소(server farm)전반의 VPN련결점들의 부하조절 즉 부하분배를 진행하는것이다. 부하조절을 위해서는 특수한 처리장치나 쏘프트웨어가 필요한데 전용부하조절하드웨어를 리용하든가 아니면 여러 VPN봉사기사이 방책복사나 상태복사를 하는 방법이 있다. 결선적인 측면에서나 경제적 측면에서나 VPN봉사기관리소를 부하조절하면 조절능력이 더 좋아 진다. 필요에 따라 더 많은 봉사기들을 추가할수 있으므로 부하조절하면 또한 예비능력도 조성된다. 그 어떤 봉사기가 고장났다면 부하를 현재 가동중인 VPN봉사기들에 분포시킬수 있다. 일부 HA(Helper Application)대안들은 접속과정을 중단시키지 않고 이런 작업을 할수 있으며 일부는 접속과정을 중단시켜야 가능하다. 암호화가속기 즉 하드웨어식암호화카드들을 VPN봉사기에 추가하여 봉사기에서의 턴넬화처리속도를 높일수도 있다. 현재 망대면부기판에 소편형태로 암호화기술이 실행되고 있다. 가속기는 턴넬이 접합되는 VPN봉사기에서 더 중요하고 대안 VPN의뢰기콤퓨터에서는 덜 중요하다.

VPN봉사기의 능력판정에서는 관리의 편리성도 고려해야 한다. 특히 관리자가 조작과제를 수행하며 자동화하는것이 어느 정도로 쉬운가 하는 문제를 제기해 보아야 한다. 실례로 새로운 턴넬을 추가하는것이 얼마나 쉬운가, 추가적인 턴넬설정파일들을 VPN의뢰기에 자동적으로 《내리먹을수》있는가 하는 물음들이다. 사용기록, 보고, 경보와 같은 기능들은 VPN봉사기관리대면부에 반드시 있어야 할 기초기능들이다. VPN사용기록이 현존 자료기지와 망관리체계에 인차 보내여 지는가, VPN봉사기가 실시간적인 사용기록과 경보를 제공하는가, 려파장치가 봉사기사용기록부에 신속히 적용되여 시간적으로 사용자선택성사건들을 강조하여 표시하는가, 수자식인증서를 사용할 때 어느 인증기관을 내세워 보증하는가, 수자식인증서 청구 및 구입절차는 자동화된 직결과정인가 아니면 사람이 수동적으로 개입할것을 요구하는가 등의 질문에 대답이 주어 져야 한다. 물론 인증서청구와 구입과 같은 반복적인 과제들은 응당 자동화되여 있기도 하다. VPN봉사기가 인증서부도명단을 요구하여 사용자인증서의 유효성을 검열해 보는가 하는 문제도 중요하다.

표 9－3은 원격접근봉사기평가기준들에 대한 례이다.

표 9-3 원격접근봉사기평가기준

- 범위성(봉사기가 결선조건들을 만족시키는가)
- 높은 리용성선택사항의 지원
- 이미 있던 사용자인증체계와 통합되는 정도
- 하드웨어식턴넬처리, 암호/복호 가속
- 사용자인증과정의 자동관리
- 운용호환성에 대한 업계VPN표준에 대한 지원
- 어떤 인증형태를 지원하는가
- 경화된 조작체계에서 VPN봉사기가 가동할수 있는가
- VPN봉사기와 의뢰기 량쪽에 설치된 방화벽의 호상결합이 가능한가
- 중앙조종화된 의뢰기관리기능
- 탁상형콤퓨터의 조작체계에 대한 광범한 의뢰기지원

인트라네트VPN

인트라네트 VPN은 기업의 광지역망(WAN)안에 있는 고정된 장소, 지사나 가정사무실들을 서로 련결시켜 준다. 인트라네트 VPN은 싸이트 대 싸이트 즉 VPN관문 대 VPN관문의 위상구조를 가진다. 인트라네트 VPN의 상업적리점은 기관의 망기반의 원가를 절약하여 정보흐름을 증가시키는것이다. 인트라네트의 본질이 싸이트 대 싸이트이기때문에 말단사용자탁상형콤퓨터에는 영향이 얼마 없다. 인트라네트를 응용하기 위하여 VPN을 판정할 때 중요하게 고려해야 할 항목은 성능, 이전망구조와의 운용호환성, 관리성이다. 인트라네트 VPN의 기술적리점은 WAN대역너비의 원가가 낮고 위상구조가 보다 유연하며(례하면 완전한 그물모양) 새로운 싸이트련결이 신속하고 쉬운것이다.

생산업체에서 제공하는 VPN하드웨어/쏘프트웨어체계들인 원격설정가능VPN기구들을 사용하게 되는 경우는 싸이트상의 관리체계나 실행시간이 없을 때이다. VPN응용제품들의 가치는 보다 전통적인 《자체건설식》방법으로 하드웨어, 조작체계, VPN봉사기쏘프트웨어를 결합시키는데 시간과 노력이 얼마나 드는가를 비교해 보면 보다 뚜렷해 진다.

전송흐름을 조절하여 어떤 규약보다 특정한 규약을 우선적으로 처리해 주는 식의 급수별봉사조절도 가능하다. 어떤 상업적요구가 제기되여 특정한 형태의 VPN전송자료가 다른 전송자료보다 회전지연시간이 적어야 한다고 하면 이때에는 이것이 문제성을 띤다. 실례로 비데오나 음성자료의 흐름식전송은 그 사용자의 기다림 혹은 그런 부류의 응용프로그람의 특성으로 하여 파일전송이나 HTTP전송보다 더 지속적인 비트속도를 요구할수 있다.

인터네트로 《굴을 뚫고 나가》는 인트라네트 VPN의 일반적사용을 제한하는 두가지 요인은 담보대역너비가 없는것과 회전지연이 있는것이다. 이 두가지 요인이 국제적으로 전개된 개별WAN식인트라네트 VPN에도 영향을 줄수 있지만 대부분의 회사들은 국제적인 개별WAN대역너비를 확보하여 인터네트상의 VPN의 낮은 원가와 경쟁할 생각을 못하고 있다. 원가 대 리윤분석을 하여 보면 개별WAN을 쓸것인가, 인터네트상의 인트라네트 VPN을 쓸것인가 아니면 외부자원을 리용한 VPN봉사를 쓸것인가를 결정하는데 도움이 될것이다. 《다중규약표식교환》(Multi–Protocol Label Switching 즉 MPLS)은 자료전송순서

를 정하는 표준방식을 제공하는 하나의 규약이다. MPLS는 회전지연을 경감시키고 담보된 대역너비문제를 해결하는데 리용된다. MPLS를 리용하면 전송자료를 분리하여 순서를 매김으로써 일부 자료들이 보다 빨리 전송되게 할수 있다. IPSec VPN응용프로그람에서 MPLS식망요소들을 사용하는 우점은 VPN전송자료가 다른것들에 비하여 우선권을 가지며 따라서 처리률이 높아 지고 회전지연이 낮아 지는데 있다.

VPN의 위상구조는 인트라네트 VPN의 경우에 중요하게 고려할 조건으로 된다. 많은 인트라네트 VPN은 그 기관의 정보흐름의 비중앙집권적인 성격으로 하여 그물 같은 위상구조를 요구한다. 다른 경우들 즉 중앙적인 정보흐름이 있거나 《중심사무실》개념을 실시해야 할 필요성이 있는 경우에는 수레바퀴식위상구조가 필요하다. 망의 변화가 부단히 진행될것으로 예상되는 경우에는 동적경로조정과 동적VPN설정을 지원하는 VPN대안이 필요하다. 동적경로조정이 필요한 경우는 사람의 간섭이 거의 없이 VPN상으로 망주소갱신을 전반적으로 빨리 해야 하는 경우이다. 경로조정봉사는 현존 망설정에 영향을 줌이 없이 강력한 대역너비관리를 할수 있는 VPN기반도 원가상 효률적으로 전환할수 있게 한다. 동적VPN기술이 필요한 경우는 VPN회선리용이 우발적이며 단시간내에만 하는것을 예견한 경우이다. 동적VPN분야에 대한 연구사업이 현재 상당히 진척되여 대규모 배비에서 VPN턴넬설치의 행정관리상 부담을 덜어 줄 전망이 보이고 있다.

인터네트를 리용하여 인트라네트VPN을 구축하는것은 일반적으로 보면 원가 대 효률이 가장 높은 VPN기술실행방법이다. 그러나 앞에서 언급한것처럼 봉사준위가 인터네트에서 대체로 담보되여 있지 않다. IP전송에 대한 봉사준위의 담보가 없지만 인트라네트 VPN에서는 다 그렇지 않다. 일부 ISP들과 개별표식 IP제공자(례를 들어 Digtal Island회사와 같은)들이 봉사준위의 담보를 제공하지만 이 기술은 이제 방금 성숙되여 가고 있는것이므로 이런 봉사제공에서 가장 큰 리득을 얻기 위해서는 고객들이 하나의 ISP의 IP망에 덧붙여 자기들의 인트라네트를 구성하여야 할것이다. 인트라네트VPN을 구성할 때 담보봉사준위, 망접근의 광범위성, 전송비용사이에서 어떤 선택안을 취할것인가를 분석해 볼 필요가 있다. 담보된 처리률준위를 요구하는 기업들은 어느 한 망봉사제공자의 개별말단간 IP망우에 자기들의 VPN을 배비할것을 고려해 보든가 가능하면 프레임중계 혹은 자기자체의 개별골간을 구축해야 할것이다.

표 9－4에는 인트라네트 VPN평가기준을 짤 때 리용할수 있는 항목들이 제시되여 있다.

표 9－4 싸이트 대 싸이트인트라네트 VPN평가기준

전제: 없음

- 자동방책분배 및 설정지원
- 그물형위상구조의 자동설정, 수레바퀴형위상구조에 대한 지원
- 망 및 봉사 감시능력
- 이질적인 망에 사용되는 경우 VPN표준의 준수
- 봉사급수조절
- 동적경로조정 및 턴넬설치능력
- 범위성과 높은 리용성

엑스트라네트 VPN

엑스트라네트 VPN은 기업동업자들과 고객들사이에서 정보흐름을 선택적으로 조종할수 있으며 여기에서 중시되는것은 높은 세밀접근조종과 강력인증이다. 례를 들어 보면 관리자는 발신자와 수신자의 주소, 인증된 사용자 ID, 사용자그룹, 인증형식, 응용형태(례: FTP, Telnet), 암호화형태, 날자시간창, 지어는 령역 등을 비롯한 다중파라메터를 리용하여 개별적응용프로그람에 사용자마다 다른 접근특권을 부여할수 있다.

엑스트라네트 VPN은 하나의 회사가 공급사슬과 기업동업자들사이에 정보를 공유하는 사용자 대 중앙싸이트모형을 리용할수도 있으며 자동망교환대(Automotive Network Exchange)와 같은 싸이트 대 싸이트모형도 리용할수 있다. 사용자 대 싸이트모형을 지향하면 사용자의 탁상형콤퓨터가 중앙싸이트의 통제밑에 있지 않는것만 제외하고는 원격접근VPN과 그 평가기준이 류사하다. 엑스트라네트사용자콤퓨터가 자기 회사의 보안방책밑에 놓이게 되기때문에 사용자콤퓨터내에서 실행되는 보안방책에서 충돌이 일어 날수 있다. 일반적으로 사용자 대 싸이트모형에서 엑스트라네트동업자들은 공동으로 노력하여 보안방책실현과 관련한 합의를 봄으로써 사용자콤퓨터, VPN의뢰기설치문제, 질문봉사안내소, 지속적인 유지보수 그리고 어느 동업자가 실수하여 다른 동업자의 망이 침해를 당하게 되는 경우 법적책임문제 등에서 안전방책실현이 촉진될수 있을것이다. 판매업체의 VPN의뢰기가 지원하는 하드웨어가동환경도 하나의 문제로서 조사하여 원격엑스트라네트동업자들이 어떤 가능한 가동환경을 쓰고 있는지 알아 보아야 한다. 대부분의 경우 엑스트라네트환경에서 선택해야 할 가장 좋은 쏘프트웨어의뢰기로서 Web접속이 사용되군 하며 SSL은 흔히 보안규약으로 리용된다. 이것으로 하여 설정과 유지보수문제가 예상외로 상당히 간단해 진다. 엑스트라네트 VPN에서는 모든 참가자들이 어느 ISP를 선택하든 괜찮은 봉사질이 제공되며 동일한 ISP를 리용해도 문제가 전혀 제기되지 않는다고 생각한다. 필요한것이란 그 그룹의 매 성원이 일정한 형태의 인터네트접근만 하면 되는것이다. 매 싸이트에 있는 VPN쏘프트웨어나 설비는 반드시 엑스트라네트의 기본싸이트에 있는 VPN설비의 IP주소로 설정되여야 한다.

엑스트라네트 VPN의 매력이 주로 시장확대능력과 기업련계능력을 강화하는데 있으므로 시장실현의 견지에서 볼 때 엑스트라네트의뢰기쏘프트웨어에 대한 상표광고 및 판매촉진사업을 할 필요가 있다고 본다. 이렇게 하자면 일부 엑스트라네트 VPN쏘프트웨어 및 봉사제공자들인 경우 엑스트라네트의 입구점으로 되는 Web페지(Web열람기를 쏘프트웨어 가동환경으로 쓰는 경우)상에서나 VPN의뢰기(전통적인 의뢰기/봉사기 쏘프트웨어모형인 경우)내에서 이 사업을 진행해야 한다. 소비자시장에서 엑스트라네트 VPN은 Web열람기식SSL의 대안으로 리용할수 있다. IPSec VPN이 Web열람기식SSL보다 더 좋은 경우는 고객이 알려 져 있으며 그 싸이트에 많이 되돌아 올수 있는 경우이다. 다른 말로 말하면 엑스트라네트VPN이 사람들이 신용카드를 가지고 구매하러 한번씩 올수 있는 소비자상품환경에서는 잘 맞지 않는다는것이다.

Web열람기식SSL은 자연발생적인 단순거래관계에서는 좋지만 고가자료접근을 필요로 하는 끊임 없는 기업관계에서는 수자식인증서식의 호상인증을 쓰는 IPSec VPN의뢰기/봉사기를 쓰는것이 더 적합할수 있다. 의뢰기측의 인증서가 사용되는 경우에는 열람기식

SSL이 적용될수 있다. 말하자는 기본내용은 수자식인증서에 의하여 사용자가 확인된다면 VPN이 접근조종기능을 리용하여 그 사용자에게 회사망에 있는 각이한 자원에 대한 접근권을 줄수 있다는것이다. 사용자들에 대한 이러한 수준의 조종이 있음으로 하여 많은 회사들에서는 이 수자식인증서를 사용하여 왔다. 분명 이것은 대규모의 엑스트라네트 VPN을 실현하는 경우에는 우려되지 않을수 없다. 엑스트라트 VPN내부에서의 PKI와 관련되는 문제들은 이 장에서 론할것이 못된다.

현존 인트라네트 VPN이 엑스트라네트 VPN실현의 기초로 리용될수 있겠는지. 그것은 위험허용수준과 보충적인 원가가 얼마나 높은가에 달려 있다. 인트라네트가 엑스트라네트의 회선들을 지원하게 하는것은 권한에 제한된 새로운 망사용자들을 정의해 주는것만큼이나 상당히 쉬운 기초적인 일이다. 그러나 자료보안에 직접 영향을 줄수 있는 엑스트라네트 VPN을 설계하는데는 일련의 미묘한 차이가 있다. 엑스트라네트를 가능한것으로 만들수 있는 방법의 하나는 가령 비무장지대를(례컨대 울타리방화벽의 3번째 대면부에) 설치하여 외부 사용자들을 지원하게 하는것이다. 이러한 방법은 인트라네트와 엑스트라네트의 자원뿐아니라 VPN봉사기를 통한 자료의 무결성과 비밀성도 방화벽이 보호해 주게 한다.

표 9－5는 엑스트라네트 VPN응용평가기준표의 례를 보여 주고 있다. 이 표에는 엑스트라네트 VPN평가기준들을 만들 때 리용할수 있는 항목표가 제시되였다.

표 9－5　　　　엑스트라네트 VPN평가기준표

- 단순통과암호/사용자이름보다 강력한 호상인증을 더 우선시한다.
- 접근조종과 사용기록이 매우 중요하다.
- 사용자주문식상표선전을 할수 있는 대안들이 더 좋다.
- 탁상형콤퓨터를 놓는 자리의 최소화(그것은 탁상형콤퓨터가 대방의것이 아니기때문에)
- 미리 설정된 VPN의뢰기와 VPN방책의 《조용한》실행
- VPN의뢰기의 사용상 편의가 관건적이다.
- 봉사준위에 대한 감시 및 사법적지원

내부망의 보안

비밀자료들이 내부 사람들에 의하여 계속 위협 당하고 있는 회사들이 최근에 깨달은 것은 VPN과 방화벽을 리용하여 내부망을 구분하거나 세분화하는것이 제품매상고에만 급급하는 보안제품판매업체들의 단순한 판매광고가 아니라는것이다. 외부의 위협이 증가하고 있는것은 사실이지만 자료보안을 위협하는 내부의 공격도 여간하지 않다. 그러므로 새롭게 부상하는 VPN대안은 내부망을 안전하게 하기 위한것으로 된다.

망보안의 견지에서 보면 망을 세분화하는데는 여러가지 방법이 있다. 한가지 방법은 내부망을 론리적으로 가르는것이고 다른 방법은 망을 물리적으로 구획하는것이다. VPN

기술은 두가지 방법을 다 리용할수 있게 한다. 실례로 목표봉사기를 VPN봉사기의 바로 뒤에 놓아 물리적구획을 지울수 있다. 여기서 목표봉사기에 접근할수 있는 유일한 방도는 VPN봉사기의 접근조종방책을 만족시키는것이다. 여기서 유리한 점은 관리가 쉽고 경계를 명확히 정의할수 있으며 접근점이 하나이라는것이다.

론리적구획화의 실례는 사용자가 목표봉사기에 접근할 필요가 있는 경우 그에게 VPN의뢰기쏘프트웨어를 제공하는 경우를 들수 있다. 사용자는 현지에 있든 먼곳에 있든 내부망의 어느 곳이든 물리적으로 위치할수 있다. VPN의뢰기쏘프트웨어는 직접 혹은 내부VPN관문을 통하여 목표봉사기와 암호화된 통화를 자동적으로 실현한다. 내부망은 결국 접근조종을 통하여 론리적으로 《구획화》되게 된다. 다른 하나의 론리적구획화씨나리오는 내부망에서 동등관계VPN통화가 실현될 필요가 있는 경우를 들수 있다. 이 경우에 필요에 따라 림시적으로 2개 혹은 그이상의 VPN의뢰기들이 VPN접속을 실현할수 있을것이다. 이러한 설정의 좋은 점은 동적VPN이 사용자의 설정조작이 얼마 없이 설치되면서도 자료의 사적비밀성이 보장된다는것이다. 이 방법의 약점은 VPN의뢰기들이 동등위치 VPN에서 강력한 사용자인증을 지원하지 못하는 경우 사용자인증강도가 떨어 질수 있다는것이다.

망계층구조안에서 어디에 VPN기능을 실현시키겠는가에 대한 위치중시에서 일련의 변화가 있는것 같다. Microsoft Windows 2000의 도입으로 하여 전용하드웨어와 쏘프트웨어를 사용하여 후에 추가하는 식이 아니라 VPN기술이 직접 조작체계에 포함되게 되였다. 이 Wondows 2000의 출현으로 하여 내부망의 안전을 보장할수 있는 VPN통합수준은 더욱 깊어 지게 되였다. VPN기술은 봉사기준위에서뿐아니라 Microsoft Windows와 UNIX의 여러 판본들에서도 실현되고 있다. 물론 이 수준의 VPN통합이 내부망보안의 전부를 의미하지는 않지만 처음부터 보안적안목의 구축을 적극 장려하는것으로 될수 있다. VPN을 목표응용봉사기에 적접 구현하는것이 현재 성능에 상당한 영향을 미치는것처럼 암호화기능을 위해서는 하드웨어가속기가 필요하다.

내부망에서 자료의 비밀성을 보장하는 문제는 원격접근VPN실행에 쓰이는 전개 및 관리방법을 꼭같이 리용하여 해결할수 있다. 사용자집단도 꼭 같다. 하드웨어가동환경도 꼭 같다. 그것은 너무나도 많은 회사들이 자기 사원들에게 무릎형콤퓨터와 같은 휴대형콤퓨터를 공급하기때문이다. 고려해야 할 하나의 차이는 물리적으로 내부망안에 있는 VPN 의뢰기에 실시해야 할 보안방책과 동일한 하드웨어를 리용하여 원격접근VPN을 통하여 원격적으로 내부망에 접근해야 할 때에 필요한 보안방책사이의 차이이다. 회사의 자료가 인터네트와 같은 공공망을 거쳐 흐르므로 비법접근의 위험성이 더 많기때문에 사용자들이 원격접속할 때에는 더 엄격한 보안방책을 실시하는것이 현명할수도 있다. 내부접근이나 외부접근이나 위험은 마찬가지이지만 원격접근 VPN을 사용할 때에는 공격 받을 가능성이 훨씬 더 크다. 내부망에 VPN기술을 적용하는 다른 하나의 목적은 LAN통신에서 자료의 비밀성을 보장하는것이다.

그러나 Microsoft File Sharing/SMB환경에서 제곱으로 증가될수 있는 VPN접속의 관리가 운영상 복잡하기때문에 일부 회사들은 단일《그룹》이나 LAN열쇠가 충분한가 하는데 대하여 조사하고 있는데 어떤 전개방식에서는 인증보다 전송할 때 자료의 비밀성이 더 중요한것이다.

내부망 VPN안전실현을 위한 평가기준의 례를 표 9－6에 주었다.

표 9－6 내부망 VPN응용의 안전을 위한 평가기준내용

- 강력한 사용자인증
- 강력한 접근조종
- 방책에 기초한 암호화에 의한 비밀보장
- 망통과시 자료의 무결성
- 내부망기반에 적은 부담을 주는것
- 사용자콤퓨터(탁상형콤퓨터)에 적은 부담을 주는것
- 편리한 관리방법
- 기성 망설비들과의 결합
- 운영비(기업목적에 대비하여 볼 때는 큰 문제가 아닐수도 있음)
- VPN의뢰기문제 :
  - 사용자투명성(사용자가 그 어떤 다른 작업을 해야 할 필요가 있는가)
  - 원격접근과 내부VPN방책사이의 차이를 자동판별하는것(VPN의뢰기가 내부/외부 보안방책변경에 자동적으로 순응될수 있는가)

VPN배비모형

이 부분에서는 네가지 VPN봉사기전개모형을 설명하려고 한다. 네가지 모형으로는 전용하드웨어 및 전용제품모형, 쏘프트웨어식모형, 경로기식모형, 방화벽식모형이 있다. VPN사용형태는 보안요구수준, 성능요구사항, 망기초시설통합노력, 실현 및 운영비 등에 따라 다르다. VPN의뢰기전개에 대해서는 앞에서 언급되였으므로 이제부터는 VPN봉사기전개문제에 대하여 집중적으로 보기로 하자.

전용하드웨어식VPN제품

현재 나오는 가장 좋은 VPN봉사기가동환경은 전용하드웨어제품 즉 특정한 용도로 만든 VPN제품의 가동환경이다. 단일용도에 최량화정도가 높은 설계로 하여(일부 측면에서) 전개, 관리, 리해가 보다 쉬우며 많은 경우 원가가 적게 들기때문에 전용하드웨어제품을 사용하는것은 매우 대중화되였다. 이러한 형태의 가동환경의 기본착상은 일반가정용품의 실례와 류사하다. 실례로 빵구이기계를 사서 집에 가져 온 다음 그것을 좀 개조해 보려고 하는 사람들은 얼마 없다. 말하자는것은 여기서 완성품인도방식을 중시해야 한다는것이다.

이 제품들은 구매자가 수정하지 않을것을 예견하여 표준하드웨어설정값으로 맞추어 판매하는것이 상례이다. 특정용도 VPN제품들은 대체로 암호화실행속도의 필요로 하여

고성능문제가 제기될 때 다른 가동환경에 비해 우월성이 있다. 대부분의 특정용도 VPN 제품들은 전용실시간조작체계상에 집적되여 있으므로 전용하드웨어에서 최량적인 가동을 할수 있게 되여 있다. 값이 눅은 많은 VPN제품들은 인텔가동환경에서 동작하는 개조된 리눅스와 BSD조작체계에서 사용한다. 대체로 이 제품들은 공장설정값으로 설정되여 먼거리에 있는곳에 운반되여 쉽게 설치되고 원격관리된다. 여기서 장점은 대규모적인 전개를 신속히 실현한다는것이다. 원격사무실이 많고 주요원거리통신사업자(telecom carriers)들을 가지고 있으며 ISP와 보안관리봉사제공자들을 가지고 있는 대규모 회사들에서는 바로 이러한 전개모형을 사용한다. 기관에 현장 IT일군들이 부족되는 경우에는 VPN제품들을 쓰면 분포도가 높은 VPN실현에서 흔히 요구되는 인적자원을 상당히 줄일수 있게 된다.

하드웨어식VPN기구들을 리용하여 분산성이 높은 대규모 VPN을 전개하는 한가지 방법은 다음과 같다. ① 기구가 쓸 기본망파라메터들을 미리 설정한다. ② VPN용품들의 수자식인증서를 미리 설치한다. ③ 용품을 원격지로 날라 간다. ④ 그다음 먼곳에 있는 사람에게 그 용품의 나머지 물리적설치를 수행하게 한다. 그 용품을 전원에 꽂은후 망케블을 련결한 다음에는 원격관리로 필요한 설정과제를 끝낼수 있게 준비되여 있어야 한다. VPN제품사용의 단점은 VPN제품하나에 모든것을 다 내장시켰기때문에 하드웨어수정을 할수 없게 된것이다. 또한 전매특허조작체계를 쓰는 VPN제품들을 리용하면 다른 또하나의 조작체계를 배워야 하며 현존 체계관리도구들과는 운용호환성이 없는 측면도 있다. 그것은 할수 없다. 자체로 VPN제품의 하드웨어를 수정하려 한다면 VPN제품방향으로 나가지 않는것이 좋을것이다.

많은 통신사업자급의 VPN교환기들 즉 수만개의 서로 다른 회선들을 관리하는 능력을 가진 VPN관문들은 대규모원거리통신망들인 전기통신회사들, 인터네트봉사제공자들이나 대기업상업망들의 요구사항에 부합되는 다른 급의 VPN부분품들이다. 통신사업자급의 VPN관문들의 특징은 설치가 빠르고 쉬우며 경험이 없는 사람도 쉽게 설치할수 있다는것이다. 업무량증대의 요구에 부합될수 있는 높은 처리률과 의뢰기쏘프트웨어가 전개하기 쉬운 점도 통신사업자급의 VPN관문의 뚜렷한 징표로 된다.

쏘프트웨어에 기초한 VPN

쏘프트웨어에 기초한 VPN봉사기들은 VPN쏘프트웨어를 일반조작체계를 쓰는 일반콤퓨터에 실치한것들이다. 지원되는 대표적인 조작체계들은 당시 시장에서 구매력이 제일 높은것이면 어느것이나 다 좋다. 이로부터 Microsoft Windows나 UNIX조작체계들은 둘다 잘 쓰인다. 일부 쏘프트웨어에 기초한 VPN들은 설치할 때 OS들을 조작하여 보안경화, 일정한 수준의 성능최량화나 망대면기판의 세밀조절 등을 하는 경우가 있다. 제품이 대체로 완성일체식으로 판매되기때문에 VPN하드웨어의 주요 부문품들의 성능을 일정하게 높이든가 《세밀조절》해 보려고 할 때 바로 이 쏘프트웨어식VPN을 리용하군 한다. 또한 현존 일반콤퓨터하드웨어를 리용함으로써 비용을 최소화하려고 하는 경우에 이 쏘프트웨어 VPN을 쓸수 있다.

쏘프트웨어에 기초한 VPN봉사기의 부족점은 전용VPN제품에 비한 성능저하, 없으면 봉사기하드웨어와 조작체계를 구매해야 하는것, 하드웨어암호화카드 구입에 드는 보충적

인 비용, 조작체계를 경화시키기 위한 보충적인 노력 등이다. 부하조절과 같은 적당한 범위성조절수법들을 리용하든가 하드웨어암호화추가카드를 사용하면 이러한 부족점들을 다어느 정도 약화시킬수 있다. 또한 VPN쏘프트웨어는 일반적으로 선불구매가격이 덜 비싸다. 때로는 쏘프트웨어가 조작체계안에 포함되여 있기도 한다. 실례로 Microsoft Windows 2000 Server에는 IPSec VPN봉사기가 포함되여 있다.

일부 판매업체들의 쏘프트웨어에 기초한 VPN제품들은 여러가지 가동환경에 쓸수 있으므로 중앙조종탁에서 관리할수 없으며 매 가동환경이 그 모양새와 느낌이 다르다. 이러한 실행과 관리에서 일관성을 보장하기 위해서는 하드웨어가동환경과 조작체계의 표준화를 진행하는것이 좋을것 같다. 가동환경의 표준화를 진행하면 새 기술습득이 최소화될수 있으며 가동환경별로 나타나는 특성들이 제거될수 있다.

경로기에 기초한 VPN

VPN을 배비할수 있는 값 눅은 하나의 입구점은 VPN기능들을 다 가지고 있는 현존경로기를 리용하는것이다. 현존 망자원들을 다 효과적으로 리용하면 실현비용을 낮출수 있으며 망관리기반시설과의 통합을 보다 쉽게 실현할수 있다. 오늘날 많은 경로기들이 VPN규약을 지원하고 있으며 보다 새로운 경로기들은 VPN전송자료들을 보다 효률적으로 처리할수 있게끔 성능이 향상되였다. 그러나 경로기의 일차적인 기능이 망사이에서 망파케트들의 방향을 잡아 주는것이기때문에 경로조정성능과 VPN기능사이에 어느것을 택하겠는가 하는것은 토론하여 결정해야 할것이다. 일부 경로기모형들은 하드웨어갱신을 지원하여 보충적인 VPN처리능력을 조성할수 있다. 현존경로기들을 갱신할수 있는 능력이 있음으로 하여 VPN사용자들이 급격히 늘어 나면 점차 그쪽으로 이행할수도 있을것이다. 많은 경로기형VPN들은 수자식인증서지원기능도 가지고 있다. 일부 경우에는 본문파일들을 자르고 붙이고 하여 수동적으로 수자식인증서 청구 및 구입을 해야 하기도 한다. VPN마디수에 따라 범위조절이 좌우될수 있다. VPN이 가능한 경로기들은 강력한 보안관리도구 즉 하드웨어제품식이나 쏘프트웨어식VPN에 흔히 제공되는것과 꼭 같은 보안관리도구들이 있어야 한다.

경로기에 기초한 VPN턴넬은 어디에서 끝나야 하는가. 두 곳중에서 어느 곳에서나 끝날수 있다. 접근경로기에 VPN을 추가할 때에는 망변두리밖에서 중단될수도 있고 혹은 내부경로기에 VPN을 추가할 때에는 방화벽뒤에서 턴넬화된 전송량을 중단시킬수도 있다.

방화벽에 기초한 VPN

방화벽은 망으로 들어 오는 전송흐름에 대하여 허용/거부결정들을 하기 위한것이다. 자기망변두리에 방화벽을 이미 설치한 회사들은 많다. 많은 방화벽들은 기능갱신능력이 있어서 VPN끝점으로 사용될수 있게 되여 있다. 그렇다면 많은 회사들에서는 자기들의 현존 방화벽이 VPN능력이 있는가를 조사해 보는것이 좋을것 같다. 이것도 현존망기반을 리용하여 초기원가를 낮추는 한가지 방법이다. 방화벽을 VPN끝점으로 리용하는데서 한가지 우려되는것은 성능이다. 망을 드나드는 모든 전송자료들이 모두 방화벽을 통과

하므로 방화벽의 부하가 과잉으로 될수 있다. 그러나 일부 방화벽판매업체들은 하드웨어암호화추가품을 제공하고 있다. 설정이 가능한 모든 보안도구에서와 마찬가지로 방화벽에도 그 어떤 변경을 해놓으면 그 보안이 다 와해된다. 방화벽에 있는 공통관리대면부를 리용하면 VPN관리가 더 잘될수 있다. 울타리방화벽으로서 한개의 점에서 진입과 탈출을 다 분리시키기때문에 이것이 리상적인 자리라고 할수 있다. VPN봉사기를 방화벽에 추가하면 하드웨어VPN, 쏘프트웨어VPN, 경로기VPN과 관련한 배치상 문제점들이 다 없어 지게 된다. 실례로 암호화된 파케트들이 방화벽에 있는 구멍을 통하여 빠져 나와야 하는가, 방화벽이 NAT(망주소변환)등을 수행하면 어떻게 되겠는가 등의 문제들이 다 없어 지게 된다.

방화벽겸 VPN방식을 도입하면 방화벽에서 VPN턴넬이 끝나며 자료복호화와 검열을 할수 있게 된다. 이 능력이 우월하다는 식의 씨나리오는 VPN턴넬을 오고가는 자료에 대하여 방화벽상주항비루스쏘프트웨어를 돌릴 필요가 있는 경우에 더욱 그럴듯하게 된다.

각종 VPN에 대한 일반관리문제

쏘프트웨어식VPN관리는 누가 해야 하는가 하는 질문이 제기될수 있다. 망운영그룹, 보안그룹, 자료소유자사이에 관리분담이 되여야 한다. 망운영문제는 망실현계획과 설계계획을 결정할 때에 반영되여야 하는데 그것은 이 그룹의 업무가 주로 회사자료의 리용성과 회사자료의 무결성을 보장하는것이기때문이다. 보안그룹은 전반체계의 설계와 능력을 분석하여 보안방책에 부합되게 해야 한다. 이 경우 자료소유자는 VPN을 리용하여 접근을 제한시키는 운영그룹을 말한다. 자료소유자는 접근조종과 사용자의 재정기록부설치를 담당할수 있다. 리상적인 조건에서 이러한 분업관계가 있으면 VPN관리에 대해서도 분담관리제를 실시할수 있다. 현실적으로 이러한 분담관리가 협조에 의하여 실현되는 경우는 거의 없다.

VPN성능평가

지금까지 말단사용자와 관리자의 견지에서 VPN을 평가하는 기준들을 보았다. 그러나 VPN판매업체들이 시장실현도구로서의 성능평가기준을 어떻게 작성하는가 하는 것을 리해하는것도 도움이 될것이다. 많은 판매업체들이 제공하는 VPN제품들을 보면 그들의 분류기준은 동시VPN접속회수, 최고통화수 혹은 처리량이다. 대부분의 보안전문가들은 그 실행이 얼마나 안전한가에 관심을 두며 대부분의 망운영성원들, 특히 ISP성원들은 VPN관문이 얼마나 많은 의뢰기나 원격사용자턴넬을 지원하는가에 관심를 가진다. IPSec원격사용자턴넬은 IKE의 암호열쇠변환 1단계와 2단계의 완성으로 정의될수 있다.

이 단계들이 완성되여야 안전한 턴넬이 형성되여 매개의 원격통화가 가능해 진다.

판매업체들은 흔히 여러가지 정의들을 만들어 자기 회사의 제품들이 최고의 성능을 발휘하는것으로 광고하기때문에 이것은 주관적인 정의이다.

많은 판매업자들이 하나의 수자를 리용하여 실지 배비에서의 VPN처리률을 특징 지으므로 조건에 따라 성능이 매우 크게 변할수 있을것이다. 다음 부분에서는 실지 현실에서 배비를 할 때 처리률에 영향을 주는 요인들을 개괄한다.

파케트크기

자료암호화와 인증과 같은 VPN의 대부분의 조작들은 파케트단위로 진행된다. CPU에서의 조종프로그람실행시간은 파케트의 크기와는 무관계하다. 따라서 파케트크기가 클수록 자료처리률수치는 더욱 커진다. 인터네트에서 IP파케트의 보통 크기는 대략 300byte이다. 대부분의 판매업체들은 상대적으로 큰 평균파케트크기인 1,000byte나 그이상에 기준을 잡고 VPN처리량특성값들을 제시하고 있다. 따라서 판매업체들에게 처리량명세에 대하여 물어 볼 때에는 넓은 범위의 평균파케트크기를 따라 가며 확정하여 예상성능을 보다 더 잘 측정하도록 해야 한다.

암호화 및 인증알고리듬

암호화알고리듬이 강하려면 더 많은 체계자원을 리용하여 수학적연산을 하여야 한다. 이때 자료처리량은 더 작아 진다. 례를 들어 DES(56bit세기)암호화에 기초한 VPN처리량은 3DES(168bit세기)암호화에 기초한 처리량보다 더 클수 있다. 스트림암호변환기는 블로크암호변환기보다 대체로 더 빠르다.

자료인증알고리듬은 자료처리량에 류사한 효과를 준다. 실례로 MD5인증은 SHA1와 비교해 보면 약간 더 큰 처리량을 나타낸다.

호스트 CPH

쏘프트웨어에 기초한 VPN방안을 리용하면 고객들이 클라스나 박자속도가 서로 다른 중앙처리장치중에서 자기가 좋아 하는것을 고를수 있다. 하드웨어식가속선택이 없는 VPN제품에서는 호스트처리능력이 특별히 중요하다. VPN을 검사해 보면 보충적인 일반CPU를 VPN봉사기에 추가해 주어도 성능이 선형적으로 증가하지 않는다는것을 알수 있다. 어느 판매업체의 주장에 따르면 Windows NT봉사기상에서 가령 하나의 중앙처리장치부하가 100%일 때 두번째 중앙처리장치를 끼워도 CPU자원은 5%밖에 덜어 지지 않는다고 한다. 또한 그 주장에 의하면 봉사기에 일반CPU를 추가하지 않고 암호화가속장치를 리용하였는데 그 처리량이 7배로 증가하더라는것이다. 다른 경우들에는 하드웨어가속에 비하여 일반용CPU를 덧붙였을 때의 가격 혹은 성능은 앞의 실례들과는 반대로 나타났다. 어느 한 경우에는 일반CPU추가원가가 하드웨어가속기값의 두배나 됨에도 불구하고 성능은 실제로 더 적게 증가하는것이였다. 속도는 CPU에 달려 있는것이 아니라 I/O모선, RAM, 캐쉬에 달려 있다. 축소명령모임(RISC)CPU들은

일반CPU보다 더 빠르며 특수용도집적회로(ASIC)들은 설계상 RISC처리장치들보다 대체로 빠르다.

조작체계와 보강준위

쏘프트웨어식VPN을 리용하게 되면 고객들은 각이한 조작체계에서 하나를 선택해야한다. 조작체계들을 사과를 비교하듯이 할수 없기때문에 고객들은 성능평가기준을 자기들의 대상조작체계에 맞게끔 주어야 한다. 또한 조작체계의 수정준위는 처리률에 큰 영향을 미칠수 있다. 흔히 최신조작체계의 보강준위로서는 더 좋은 성능을 낼수 있게 된다. 만일 VPN요구사항이 조작체계형VPN기술을 쓸것을 요구한다면 대부분의 쏘프트웨어방화벽들이 그러하듯이 필요한 조작체계의 《경화》를 수행하는 쏘프트웨어제품들을 고려해보는것이 좋다. 갱신판프로그람, 보안경보, 수정갱신판을 제공하는 봉사체계에 가입하는것도 고려해 볼수 있다.

망대면부기판구동기

망대면부기판(NIC)판본도 처리률에 영향을 줄수 있다. 흔히 최신판 망대면부기판구동기들은 성능이 가장 좋다. 현재 수많은 망대면부기판제작업체들은 IPSec형VPN들에 보완적인 기능을 수행하는 제품들을 내놓고 있다. NIC를 사용자콤퓨터나 암호화와 복호화를 수행하는 IPSec VPN관문에 설치하면 CPU사용률은 낮추면서도 체계성능은 높일수 있다. 이렇게 하려면 NIC에 직접 처리장치하나를 설치해야 NIC가 망전송량처리의 대부분을 맡아 수행함으로써 호스트체계가 봉사응용프로그람에 더 집중할수 있게된다.

기억기

VPN이 원격사용자턴넬별로 범위조절을 할수 있는 능력은 관문봉사기에 설치된 체계기억기의 용량에 달려 있다. 많은 VPN용품(이것들은 고정된 용량의 기억기를 가지고 있음)들과는 달리 쏘프트웨어형VPN들은 핵심부에서의 최고동시접속수에서 한계가 있으므로 동시회선지원과 원격사용자턴넬에서 제한을 받는다. 일부 경우에는 동시접속이 VPN응용 대리자접속한계에 의해 제한되기도 하는데 이것은 호스트핵심부한계와는 무관계하다. 그러나 대부분의 VPN전개에서는 접속한계수자에 도달하기전에 벌써 처리량한계에 부닥치군 한다. 쏘프트웨어에 기초한 VPN가동환경의 기억기확장성과 전용하드웨어의 처리상 우점들을 잘 결합하여야 량자의 최상의 효과를 기대할수 있다. 다음의 가상적인 실례를 고려해 보자. 어느 한 기관이 하드웨어가속기가 설치된 쏘프트웨어식VPN에 30Mbps의 인터네트를 접속시켰다. 이 기관에서는 원격사용자 한명당 필요한 평균자료속도는 대략 40K이다. 이 씨나리오에서 VPN은 대략 750명의 원격사용자를 동시지원할수 있다. 일단 사용자수가 750명이상으로 오르면 평균자료속도와 해당 사용자의 사용률은 떨어 지기 시작할것이다. 여기에서 명백한것은 믿음직한 동시사용자지원이

제한 받게 되는것은 접속수의 한계가 아니라 쏘프트웨어식VPN관문의 처리률때문이라는것이다. 이런 관점에서 보면 쏘프트웨어식VPN배비에서 규모조절을 하여 수천명의 사용자를 동시에 처리할수 있게 하는데서 관건적역할을 하는것은 바로 암호화가속카드이다.

수자 하나만 가지고서는 VPN의 처리성능을 정확히 측정할수 없다. 실례로 VPN에서 전송되는 파케트의 크기는 처리률에 큰 영향을 준다. 파케트크기가 작으면 체계성능이 떨어 진다. 파케트크기가 작을수록 호상 더 많은 수의 파케트들이 처리되고 간접비는 더 높아 지며 결국 효과적인 처리량은 더 낮아 진다. 암호화가속카드는 큰 파케트와 작은 파케트를 다 동조하여 처리할수 있으므로 모든 파케트크기들에 한하여 다 성능이 최량화된다. 성능에 영향을 주는 다른 요인들로서는 체계설정(CPU, 기억기, 캐쉬 등), 암호화알고리듬, 인증알고리듬, 조작체계, 전송형태 등이 있다. 이 대부분의 요인들은 모든 VPN제품들에서도 마찬가지이다. 따라서 경쟁적인 VPN제품들에 있는 성능명세를 보고 그 수값들을 모든 환경에서 직접 현실값과 비교하거나 실지적인것이라고 생각하면 안된다.

자료압축

성능을 대폭 올리고 말단사용자들이 만족감을 가지게 하려면 VPN에서의 속도지연을 최소화하여야 한다. 지연최소화방도는 적은 전송량을 보내는것이다. 이렇게 하려면 VPN상에 보내기전에 자료를 압축해야 한다. 압축으로 인한 성능증가는 어떤 자료를 보내는가에 따라 달라 진다. 그러나 일반적으로 자료가 일단 암호화되면 압축되지 않으므로 암호화하지 않는것이 낫다. 자료압축은 특히 낮은 대역너비의 상사형전화회선VPN접근을 최량화할 때에 성능향상에 매우 중요한 역할을 한다. 이때 MTU(최고전송속도)의 크기와 쪼각화가 주요원인으로 될수 있다.

원래성능이 가장 중요한 기준일가

VPN평가에서 사용자들이 어느 특성들을 가장 중요시하며 앞으로 나오는 제품에서 무엇을 바라는가를 밝혀 내기 위하여 진행한 최근의 VPN사용자조사자료에 의하면 VPN평가에서 보안보다 성능이 더 높은 요구로 제기되고 있다는것이 밝혀 졌다. 이것은 VPN기초기술의 보안에 대하여 믿는 사람이 얼마 없던 초기 VPN시기로부터 사고방식이 완전히 달라졌음을 보여 주는것이다. 특히 VPN기술과 제품에 대한 신뢰도가 《높은》것으로 평가하는 보안전문가들속에서 그런 관점이 지배적이다. VPN을 잘 알고 있는 사람들은 보안제품들에 대하여 신뢰성을 가지고 있으며 성능과 관리는 다음의 큰 문제라고 보고 있다. 보고서자료에 의하면 기본보안부분품들이 우려되고 있지만 그렇다고 하여 VPN성능이 절대로 희생되여서는 안된다고 사용자들이 주장하고 있다고 한다. 또한 조사에서 밝혀 진데 의하면 사용자들이 많은 관심을 돌리는것은 성능, 실행보안 및 리용성과 같은 높은 급의 요구들이며 적게 관심돌리는것들은 VPN의 기본기술과 규약이라고 한다.

VPN에 대한 외탁(Outsourcing)

외부의 지식 있는 봉사제공자에게 위탁하면 말썽거리가 생겨도 전문가가 있어 일 없겠다는데로부터 일정한 안전감을 가지게 된다. 외탁 즉 외부의 자원을 리용하면 자기 회사의 보안관리자들은 지사들이 망에 추가할 원격사용자들을 설치 및 시험할 때마다 VPN을 물리적으로 갱신하느라고 애 쓰지 않아도 된다. 자기회사에 지역적으로 널려 진 기관망이 없는 경우에는 VPN의 통과점만 인터네트봉사제공업체나 개별IP망제공업체에 외탁하면 될것이다. 그러나 일반 인터네트접속이 되였다 하여 VPN상 전송량이 최대부하시간에 인터네트상의 전송량과 합쳐 져 막힘현상이 일어 나지 않으리라고는 크게 확신할수 없는것이다. ISP나 VPN봉사제공자들은 필요한 하드웨어와 쏘프트웨어를 선정하여 설치할뿐아니라 기술봉사와 지속적인 유지보수임무를 훌륭히 수행하여야 한다.

표 9−7은 VPN봉사제공자평가에서 고려해야 할 일부 요인들을 제시하고 있다.

표 9−7 VPN봉사제공자평가항목

VPN봉사제공자평가시 고려해야 할 요인들은 다음과 같다.

- 봉사의 질
- 신뢰도
- 보안정도
- 관리능력
- 봉사제공자 자체망과 망관리쎈터의 보안상태
- 봉사제공자의 인원채용관례에 대한 조사(전문지식, 신원조회)
- 봉사제공자는 VPN배비를 전후하여 어떤 봉사를 제공하는가(취약성평가와 토론봉사)

신뢰도

사용자들이 망에 들어 가지도 못하며 접속도 제대로 안된다면 보안이라는것은 무의미하다. VPN의 목적이 이동근무자들에게 원격접근을 제공하는것이라면 성능의 기본측면은 봉사제공자가 해당 봉사지역내에 얼마나 많은 호상 접속점들을 가지고 있는가에 따라 평가될것이며 이것이 또 전화회선시 접근의 성공률이 얼마인가를 담보하는것으로 될것이다. 실례로 어느 VPN봉사제공자(전송 및 보안봉사제공)가 97%의 접속률을 가진 전화회선식원격접근을 제공하는데 초기모뎀련결속도는 26.4KB/s이상이며 시간보장률이 99%라고 한다. 다른 VPN봉사제공자(전송 및 보안봉사제공)는 100%의 망리용률, 전화회선식봉사의 95%의 접속성공률을 보장한다. 이러한 담보가 맞지 않으면 봉사제공자는 대체로 일종의 재정적보상이나 봉사신용을 약속한다. VPN통신 및 보안봉사는 각각 따로 외탁할수 있다.

그러나 회사에 넓은 지역망봉사가 기본목표라고 한다면 전반적망의 리용률과 속도가 주되는 관심사로 될수 있다. 봉사제공자들은 현재 전반적망의 평균값들을 기초로 하여 처리률, 회전지연시간, 리용성 등과 같은 일정한 수준의 성능을 담보하는 방법으로 이 문

제를 대처하고 있다. 자체의 기관망을 구축하는 봉사제공자들은 그것을 리용하여 많은 고객VPN을 지원하고 있다. 일부 VPN봉사제공자들은 비동기전송방식이나 프레임중계식 전송을 통하여 고객VPN에 개별WAN봉사를 해주고 있다. 이렇게 VPN전송은 일반인터네트전송과 대역너비싸움을 할 필요가 없으므로 VPN봉사제공자들은 망의 끌점 대 끌점성능을 관리하는 사업이나 잘하면 된다.

봉사의 질

VPN봉사제공자들이 최근에 성능담보를 시작하는 분야는 성능에 예민한 전송자료들인 육성자료와 다매체자료들이다. 실례로 망에서 비데오자료는 고속전송해야 쓸수 있으므로 일반 파일전송보다 비데오전송에 더 큰 우선권을 부여할수도 있다. 현재 난점은 망경계를 넘어서 이 담보를 할수 있겠는가 하는 문제이다. 단일한 망을 통하여 자료전송이 현재 가능한것만은 사실이지만 여러개 망을 거쳐야 하는 경우는 어쩔수 없다. 그것은 MPLS와 같은 표준들이 나오고 있지만 인터네트는 더 말할것도 없고 일반적인 망에서조차 현재 전송자료의 순위를 정하는 단일한 규정이 제시되여 있지 않다.

더 좋은 성능을 담보하기 위하여 많은 VPN봉사제공자들은 봉사준위의 협정들을 체결하고 있다. 봉사의 질에 해당하는 추가료금지불을 위하여 VPN봉사제공자들은 처리량, 전화회선접속, 망리용률에 대한 담보를 고객들에게 제공할수 있다. 일부 VPN봉사제공자들은 자체의 프레임중계나 비동기전송방식망들을 제공하여 VPN전송량을 거기에서 경로조정함으로써 성능을 높이고 있다.

보안

VPN에서는 암호화, 턴넬화, 인증 및 권한부여를 적절히 결합함으로써 보안을 보장한다. 방화벽은 신뢰성 있고 허용된 합법적인 파케트나 사용자들만 회사망에 접근시킴으로써 회사내 보안방어를 보장한다. 회사들은 자기들의 VPN보안방법을 VPN봉사제공자가 선택하도록 할수 있으며 그 관리를 회사자체로 하든가 아니면 봉사제공자가 그 관리기능을 수행하게 할수도 있다. 다른 방도로서는 고객이 자체로 VPN전반에 대한 보안방책을 정의하게 할수도 있다. 대부분의 보안관리자들은 자기들의 망보안에 대하여 일정한 정도의 통제권을 보유하는것을 더 좋아 하는데 그것은 주로 말단사용자에 대한 관리, 방책 및 인증분야이다. 회사들은 자체암호화를 선택할수도 있으며 자체보안봉사기를 운영할수도 있으나 감시나 경보대응과 같은 기타 VPN관리문제들은 VPN봉사관리자들을 시켜서 처리할수도 있다. 보안관리와 관련하여 외탁을 하겠는가에 대한 결심채택은 회사의 규모와 IT자원의 규모에 달려 있다. 일부 회사들의 경우 외탁결심채택은 회사의 자료의 비밀적성격과 외탁에 대한 IT관리자들의 신뢰도와 더 많이 관련되여 있다고도 볼수 있다(표 9−7 참고).

관리능력

고려해야 할 또하나의 문제점은 VPN봉사제공자에게 필요한 관리능력과 보고능력이

다. 많은 VPN봉사제공자들은 가입자들에게 망성능자료와 고객사용률보고서에 일종의 Web접근을 할수 있게 한다. Web도구들을 쓰면 사용자들은 원격설정, 사용자추가 및 삭제, 갱신을 진행하는 문제, 수자식인증서발급을 통제하는 문제, 성능준위자료감시 등과 같은 문제들을 자체로 수행할수 있다. 고객들이 사용자추가 및 삭제를 하며 높은 급에서 방책변경을 제기할수 있게끔 관리가 분할된 제품을 VPN봉사제공자가 제공할수 있는가 없는가 하는것도 알아 보아야 한다.

요 약

VPN평가전략을 잘 세우면 보안전문가들은 제작업체가 가장한것과 실지 성능지표들을 갈라 내여 회사자체의 VPN체계에 대한 요구를 보장할수 있게 될것이다. 기본은 필요한 VPN실현형태에 부합되는 전략과 기준들을 설정하는것이다. 평가기준들에서는 필요되는것들에 대한 정의를 정확히 주어야 한다. 실천적으로 검증된 실험실조건에서의 평가를 하면 어떤것을 가져다 써야 하는가를 보안전문가들이 정확히 알게 될것이다. VPN설치에 대한 세부 사항들에 주의를 돌려야 하며 선정된 VPN봉사제공자나 제품판매업체에 대한 경각성을 높여야 한다.

또한 VPN전개전략을 심사숙고하여 짜게 되면 실현비용을 낮추고 사용자들의 호평을 높이게 되며 투자률, 수익률을 가속화할수 있다. 전개전략은 VPN응용형식과 VPN배비모형을 어떻게 선택하는가에 따라 달라 질수도 있다.

전통적으로 보면 판매업체들이 추구하는것은 고객들에게 선택항목들을 될수록 적게 주어 판매주기를 간소화하는것이다. 그 방도의 하나로서 VPN제품의 성능특성값들을 극히 간단하게 해놓는것이다. 작은 규격, 중간 규격, 큰 규격중에서 어느것을 사렵니까? 10명의 사용자가 쓰는 VPN봉사기, 100명용봉사기, 1,000명용봉사기중에서 어느것을 사렵니까? 100MHz 아니면 1Gbit모형을 사렵니까? 이런 질문들이 제기된다. 판매업체들에서 자기 주장을 정당화하는데 필요한 파라메터들을 제공하겠으면 제공하라고 하라, 중요한것은 보안전문가들이 판매업자들이 쓰는 특정성능값들과 평가방법론들을 알면 되는것이다. 이러한 지식들을 알고 있으면 보안전문가들은 제품선택에서 정확한 결심채택을 할수 있을것이다.

VPN을 실현하는데는 많은 방도들이 있을것이다. 보안관리봉사제공자들은 일부 부담을 덜고 VPN실현을 신속하게 도와 줄수 있을것이다. 그러나 보안전문가들은 봉사제공자선택에서 응당한 성실성을 발휘하기 위하여 적극 노력해야 할것이다.

용어해설

ATM(Asynchronous Transfer Mode) 비동기전송방식

초고속능력의 수자통신수단으로서 자료전송뿐아니라 영상, 음성 및 비데오전송에 적합하다. 주로 기관망에서 리용된다.

DSL(Digital Subscriber Line) 수자식가입자선로

경쟁적인 지역교환통신회사들과 지역전화회사들이 자기의 가입자들에게 광대역접근을 제공하는 고속수자식선로들의 총칭

FTP(File Transfer Protocol) 파일전송규약

사용자들이 자기의 현지 콤퓨터와 망상의 임의의 체계사이에 파일을 복사할 수 있게 하는 규약으로서 여기에는 FTP의뢰기와 FTP봉사기 두가지가 있다.

IKE(Internet Key Exchange) 인터네트암호열쇠교환규약

IPSec VPN통화시 사용하는 보안파라메터(보안련계라고도 함)들을 구축하는데 쓰이는 규약

IPSec(IP Security Protocol) IP보안규약

VPN에서 사용되는 표준규약묶음으로서 암호화 및 자료무결성알고리듬들과 규칙들을 정의하여 안전한 IP파케트의 형식과 전송을 규제해 준다.

Kbps(Kilobits per second) 초당키로비트

Mbps(Megabit per second) 초당메가비트

MSP(Managed Security Service Provider) 보안관리봉사제공자

고객들을 대표하여 각이한 망보안과제들을 맡아 수행해 주는 봉사제공자나 봉사제공업체의 한 부류이다. VPN봉사제공자들은 VPN봉사기/의뢰기전개를 방조하며 VPN의 운영관리를 맡아 해준다.

SSL(Secure Socket Layer) 안전소케트층규약

Netscape 회사가 원래 개발한 안전규약이다. SSL은 의뢰기와 봉사기사이의 전송을 인증하고 암호화하여 진행함으로써 WWW에서 보편적으로 인정되여 왔다. SSL은 흔히 FTP와 같은 다른 TCP/IP를 안전하게 하는데 사용될수 있지만 주로 열람기에서 쓰인다. SSL은 TLS로 전환되였다.

TLS(Transport Layer Security Protocol) 전송층보안규약

IETF가 제안한 표준규약초안으로서 인터네트상에서 통신의 사적비밀을 보장하는데 쓰인다. 이 규약을 리용하면 의뢰기/봉사기에서 도청, 조작, 통보문위조를 방지하게끔 할수 있다.

VPN client VPN의뢰기

개별적인 사용자콤퓨터에 상주하며 VPN턴넬을 구성하여 VPN봉사기로 접속하게 하는 쏘프트웨어이다.

VPN server VPN봉사기

중앙위치에 상주하여 VPN턴넬을 종결시키는 장치(IPSec보안관문)이다.

VPN의뢰기와 다른 VPN봉사기와 통신을 한다. 쏘프트웨어식일수도 있고 하드웨어식일수도 있다.

VPN(Virtual Private Network) 가상개별망

자료의 비밀성, 인증, 자료무결성을 보장하여 자료를 전송할수 있는 능력을 가진 망이다.

제１０장. Checkpoint방화벽보안점검을 어떻게 할것인가

벤 로드커

《변경된 상태》는 인간의식의 변경된 상태를 시험하는 과학자에 대한 단순한 과학환상영화가 아니였다. 이것은 대기업들이 가지고 있는 많은 방화벽에 대하여 표현한 말이기도 하다.

일반적으로 방화벽이 처음으로 구축되면 그 기관의 보안요구사항은 엄격해 진다. 집단적환경에서 쓰게 되면 방화벽의 규칙기지, 설정상태, 주요조작체계들이 완전히 다른 형태들로 변화되기 쉽다. 이 변경된 방화벽상태는 방화벽점검을 필요로 한다.

방화벽은 설정의 정확성정보만큼 효과를 나타낸다. 오늘날의 집체적환경에서 방화벽의 설정상태는 나빠지기가 일쑤이다. 방화벽설치상태를 점검해 봄으로써 경영진은 이 방화벽이 예견한대로 안전하게 자기의 역할을 하고 있는가를 확인할수 있을것이다.

이 장에서는 Checkpoint의 Firewall–1에 대하여 방화벽점검을 하는데 초점을 둔다. 이 내용들은 그 대부분이 Cisco PIX, NAI Gauntlet, Axent Raptor 등 그 어느 방화벽에나 다 긴밀한 련관이 있을 정도로 상당히 보편적인것들이다. 그러나 한가지 경고할것이 있다. 즉 여기서 중요한것은 방화벽점검이 결코 침투시험은 아니라는것이다. 방화벽을 점검하는 목적은 남의 약점을 찾아 내여 방화벽을 뚫고 들어 가자는데 있는것이 아니라 방화벽의 실수로 열어 놓은 구멍들과 위협요소들을 찾아 내자는데 있다.

마지막으로 방화벽점검 역시 방화벽조작체계나 주요망조작체계가 완전히 안전하다는것을 확인하거나 보증하는 과정이 아니라는것도 충분히 알아야 한다.

방화벽점검의 필요성

방화벽도 사람과 같아서 점검해 보아야 한다. 일터에서는 이것을 사업능률점검이라고 하며 의학분야에서는 이것을 검진이라고 한다. 정기적으로 방화벽을 점검하는것은 필수적요구이다. 그것은 설정이 잘못된 방화벽은 방화벽이 없는것보다도 더 못하기때문이다. 방화벽이 없으면 위험이 조성되며 근본적인 보안대책이 없다고 생각한다. 그러나 설정이 잘못된 방화벽을 가지고 있으면 보안이 잘되고 있는것처럼 잘못생각할수 있게 된다.

보충적으로 말하여 방화벽은 흔히 제1차적인 정보보안체계이므로 방화벽에 그 어떤 결함이나 설정상 오유가 있으면 전반적기업에 그것이 큰 영향을 미친다는것이다. 방화벽점검을 전혀 하지 않으면 이러한 결함들이 퇴치되지 않은채로 남아 있게 된다.

점검, 검열 및 평가

방화벽점검을 흔히 검열이라고 한다. 검열이란 《차례차례 구체적으로 조사하여 총화해 보는것》이라고 정의한다. 점검, 평가, 검열 등의 단어들은 흔히 동의어적으로 쓰인다. 북아메리카의 5대 회계회사들에서 무은 보안그룹이 보안점검을 할 때면 흥미있게도 그들은 《감사》라는 말을 쓰게 되여 있지 않다고 한다. 그 리유는 이 5대회사들을 감독하는 공공회계연구소(www.aicpa.org)가 해당 환경에서 검열을 진행할만한 공식적인 정보보안표준제도가 없다고 하면서 《검열》이라는 용어를 쓰지 못하게 하였다는것이다.

한편 재정검열은 일반공인회계원칙(GAAP)에 어긋나게 진행되고 있다. 고정된 규정은 아니지만 GAAP는 재정정보를 보고하기 위한 널리 인정된 관례, 기준 및 절차의 틀거리이다. 재정회계규정위원회(www.fasb.org)는 1973년에 이 GAAP를 작성하여 내놓았다. 이 재정회계규정위원회의 사명은 재정정보의 발행인, 검열원, 사용자들을 비롯한 사회일반사람들을 지도교육하기 위한 재정회계 및 보고에 대한 규정을 작성하고 개선하는것이다.

2001년 1월 현재 일반공인체계보안원칙(GASSP)위원회는 국제정보보안재단(IISF)을 설립하고 재정을 보장하기 위한 계획이 담겨 진 업무초안을 작성하는 기초단계를 거치고 있다. 현재는 일반적으로 공인된 한조의 보안방책도 없지만 이러한 규정을 작성하기 위한 사업이 지금 진척중에 있다. 그 재단을 연구완성하기 위한 사업과 GASSP의 틀거리를 문안작성하고 승인하기 위한 사업도 현재 진행중에 있다. 이 위원회는 GASSP세부원칙을 마무리하기 위한 하나의 세부계획과 IISF자금조달이 진행되면 즉시 그 계획을 실행하기 위한 안을 개발하여 놓았다.

GASSP가 없으면 하부구조의 보안유지를 위한 권위 있는 법적기초가 없게 된다. GASSP 같은것이 있다면 일정한 정도의 법적준수를 실시하고 그에 기초하여 근거가 합당한 GASSP의 례외조항 혹은 리탈조항들을 공식적으로 승인해 줄수 있는 방도가 나설것이다.

GASSP와 리론적으로 류사한것은《공통표준계획》(http:// csrc.nist.gov/cc)이다. 공통표준은 국제적인 규모로 진행되는 개발계획으로서 정보기술제품과 체계들의 보안적특성을 최종평가하는 방법의 하나이다. 이러한 공통표준기지를 구축하면 정보기술보안평가의 결과가 보다 광범한 사회계에서 더욱 설득력 있게 될것이다.

공통표준은 개별적인 보안평가결과들을 서로 비교할수 있는 조건도 마련해 줄것이다. 정보기술제품 및 체계의 보안적기능과 보안평가를 진행할 때 이 제품 및 체계에 적용할수 있는 품질담보대책에 대한 공통적인 요구사항들을 제시하면 이 비교가 더 쉽게 될수 있다. 이러한 보안평가과정이 진행되면 이러한 제품 및 체계의 안전기능과 담보대책이 이 요구사항들에 부합된다는 일정한 정도의 신뢰도가 조성된다. 평가결과를 보면 정보기술제품 및 체계가 목적한바대로 안전한가 그리고 사용에서 있을수 있는 보안상 위험요소들이 허용할만한것인지에 대한 결심이 설것이다.

방화벽점검단계

방화벽구조, 안전대책안 그리고 공정에 대한 전반적인 점검의 내용은 다음과 같다.

- 기초시설에 접근하는 종업원 및 거래대상자들의 기초시설접근을 규제하는 절차들
- 기초시설의 물리적 및 론리적구조
- 기초시설의 하드웨어 및 쏘프트웨어의 판본들과 주요망조작체계
- 접근조종정보에 대한 기초시설적통제수법들
- 사용기록부에서의 사건선택과 통지기준들
- 보수 및 행정적관리를 위한 접근까지 포함한 일체 접근경로들
- 보안방책 및 대책들과 행정적절차(즉 사용자 및 봉사의 추가와 삭제, 설비 및 체계검사기록부의 검열, 체계와 매체의 보유 등)
- 사용자구좌, 파일체계허용사항, 실행파일속성, 특권프로그람들, 망쏘프트웨어 등 망조작체계 전반에 대한 접근조종
- 침입, 봉사거부공격 등이 일어 날 경우에 대처한 기초시설에 대한 비상대응계획내용
- 게재된 보안경보게시판에 대한 접근과 사용

방화벽점검을 진행할 때 여러가지 방법들을 리용할수 있다. 다음의 여섯가지 단계를 중심으로 대부분의 점검이 진행된다.

- 기초시설과 그 구조를 분석한다.
- 기관의 방화벽방책을 검열한다.
- 호스트들과 망분석스캔을 동작시켜 본다.
- Firewall–1의 설정상태를 검열한다.
- Firewall–1의 규칙기지들을 검열한다.
- 이 모든것들을 보고서에 반영한다.

다음의 사항들로 매 단계를 확장해 나간다.

1단계: 기초시설과 그 구조를 분석한다.

방화벽이 망보호를 제대로 하는가를 알려면 망기초시설을 리해하는것이 필요하다. 점검하여야 할 항목들은 다음과 같다.

- 인터네트접근의 요구사항들
- 인터네트 혹은 인트라네트 접근의 업무적정당성에 대한 료해

- 허용되여 들어 오는 봉사와 나가는 봉사 형태들에 대한 확인
- 방화벽설계(즉 dual–homed, multi–homed, proxy)의 검토
- 내외부망과의 련결상태분석
  - 울타리망과 외부와의 접속
  - 전자상업거래관문
  - 회사내 및 회사들사이의 LAN–WAN련계
  - 전반적회사의 보안구조
  - 해당 장소에 있는 전체 콤퓨터시설물
- 망관리자들과 방화벽관리자들과의 담화

정보보안구조에 결함이 있어 회사의 방책이 반영되지 못하였다면 방화벽이 그 부족점을 절대로 메꾸어 줄수 없다.

방화벽의 견지에서 볼 때 규모조절이 가능하고 분산화가 가능한 방화벽체계를 구성하기 위하여 Checkpoint회사는 Firewall–1제품의 기능을 두가지 구성요소로 즉 방화벽모듈과 관리모듈로 갈랐다. 이 두 구성요소들사이의 호상작용에 의하여 표준Checkpoint방화벽구조전체가 구성되는것이다.

관리모듈은 다른 모듈들에 대한 중앙적인 조종을 하게 되며 방화벽의 기능들을 규제하는 규칙들과 대상들이 있는 곳이다. 다른 방화벽모듈들이 생성하는 모든 사용기록부와 경고문들이 이 관리모듈에 집중되여 보관되고 문의되고 점검되게 된다.

방화벽모듈자체는 서로 다른 구역간에 교환되는 전송자료가 실지 통과하는 관문체계이다. 방화벽모듈은 파케트들을 검사하고 규칙들을 적용하며 사용기록부와 경고문들을 생성하는 체계이다. 방화벽모듈은 하나 혹은 그이상의 관리모듈에서 규칙기지들을 참조해 보며 사용기록부에 보관하지만 관리모듈이 가동하지 못할 때에는 자기자체의 현재 규칙기지를 참조하며 독립적으로 기능을 계속 수행할수도 있다.

방화벽구조설계에 리용할만한 가장 훌륭한 참고서는 Elizabeth Zwicky가 쓴 *Building Internet Firewalls* (O, Reilly & Assoc ISBN: 1565928717)이다.

2단계: 기관의 정보체계의 보안방책을 검열한다.

방책은 방화벽을 효과적이며 성과적으로 운영하는데서 사활적인 요소로 된다. 방화벽은 사용과 관리를 규제하는 실지사업적인 방책의 견지에서 구축되지 않는다면 효과를 나타낼수 없게 된다.

마크스 라눔은 방화벽이란 《인터네트보안방책의 실현이다. 만일 보안방책을 가지고 있지 않으면 방화벽을 가지고 있지 않는것이나 같다. 반대로 그 무엇인가 있으면 그것은 그 일을 하는것이라고 볼수는 있다. 그러나 다른 사람이 그 일을 이렇게 해야 한다고 말해 주지 않으면 실지 그것이 무슨 일을 해야 하는지 알수 없게 될것이다》라고 말하였다. 이런 견지에서 어떤 기관이 정해 진 방화벽방책이 없는 상태에서 방화벽점검을 잘하려고 생각한다면 그것은 그 기관의 미숙한 상태에서 그 무엇을 깨달으려고 하는것으로밖에 될수 없다.

방화벽을 점검할 때 방책에 기초하여 제기할 일부 질문사항들은 다음과 같다.

- 기관에서 발표된 방화벽방책이 있는가.
- 최고경영진이 방화벽기초시설과 관련한 방책들을 검열하고 승인해 왔는가.
- 기관의 정보보안통제는 누가 책임지고 있는가.
- 방화벽방책을 변경시킬수 있는 절차들이 있는가, 있다면 공정은 어떤가.
- 이러한 방책들이 기관내 전체 성원들에게 어떻게 통과되는가.

방화벽의 관리에 대하여 제기할 문제점들은 다음과 같다.

- 방화벽들은 누가 소유하고 있으며 그것이 규정되여 있는가.
- 매개 방화벽에 해당한 방책실행은 누가 책임지고 있는가.
- 방화벽에 대한 일상적인 관리는 누가 책임지고 있는가.
- 방화벽사용과 관련한 방책준수정형은 누가 감시하고 있는가.
- 보안관련사건은 해당 정보보안관계자들에게 어떻게 보고되고 있는가.
- 새로운 취약점들의 존재에 대해 CERT나 CIAC 등 판매입체 등 판매업체마다 고유한 자문을 감시하는가.
- 내적해결 및 보고 등 각종 사건에 어떻게 대응해야 하겠는가에 대한 서면으로 된 절차는 있는가.

변경통제는 방화벽에서 사활적인 문제이다. 일부 변경통제와 관련한 문제점들은 다음과 같다.

- 변경통제절차에 대한 문건이 있어야 한다.
- 시험계획들이 총화되여야 한다.
- 갱신설정절차를 점검한다.
- 경영진의 승인과정을 점검한다.
- 다음의 구성요소들에 대한 변경내용이 문건화되였는가를 점검한다.
  - 판본갱신이나 부분보충/수정시 가동정지시간을 통지하고 계획화해야 한다.
  - 모든 변경내용에 대한 전자적인 복사판들
  - 모든 변경내용에 대한 종이문건기록

마지막으로 재난발생시 예비본(backup)과 비상대책계획이 필수적이라는것을 고려해야 한다. 일부 문제점들은 다음과 같다.

- **Firewall–1프로그람의 《황금본》을 보관해 둔다** 황금본(golden copy)이란 호스트가 망과 련결되기전에 만들어 놓은 총적인 예비본을 말한다. 이 예비본을 복구할 때 리용할수도 있고 방화벽이 일정하게 의심을 불러 일으키는 경우 참조해 볼수도 있다.

- **예비본작성절차와 해당 문건들을 점검한다** 예비본작성절차에는 복원절차가 포함되여야 한다. 즉 예비본을 작성한후에 복원해 보아서 그 전일성이 확인되여야 예비본이 완전한것으로 될수 있다. 또한 예비본들이 안전한 곳에 보관되여야 한다(주의: 강조할것은 많은 경우 금고가 예비본매체를 물리적으로 보존할수는 있지만 화재때에는 열에 의한 파괴를 어쩔수 없다는것이다. 테프, 플로피, 하드디스크 같은 자료매체를 보존하기 위하여 금고를 특수하게 설계해야 한다.). 방화벽을 다시 구축하거나 교체해야 할 경우에는 여러 파일들을 복원하여야 한다(표 10－1). 이 파일들은 테프구동기나 기타 큰 보관도구와 같은 외부적인 구동기를 리용하여 체계완전예비본을 통하여 작성될수 있다. 방화벽기능을 실현하는데 가장 사활적인 파일들은 플로피디스크 한장에 들어 가게끔 해야 한다.

표 10－1　예비본을 따두어야 할 Firewall–1의 기본설정파일들

관리모듈에서

$FWDIR/conf/fw.license
$FWDIR/conf/objects.C
$FWDIR/conf/*.W
$FWDIR/conf/rulebases.fws
$FWDIR/conf/fwauth.NDB*
$FWDIR/conf/fwmusers
$FWDIR/conf/gui–clients
$FWDIR/conf/product.conf
$FWDIR/conf/fwauth.keys
$FWDIR/conf/serverkeys.*

방화벽모듈에서

$FWDIR/conf/fw.license
$FWDIR/conf/product.conf
$FWDIR/conf/masters
$FWDIR/conf/fwauth.keys
$FWDIR/conf/product.conf
$FWDIR/conf/smtp.conf
$FWDIR/conf/fwauthd.conf
$FWDIR/conf/smtp.conf
$FWDIR/conf/fwauthd.conf
$FWDIR/conf/fwopsec.conf
$FWDIR/conf/product.conf

$FWDIR/conf/serverkeys.*

www.phoneboy.com/fwl/faq/0196.html을 보라.

- 예비본작성시간표를 점검한다.
- 절차가 준비되여 있어서 봉사가 파탄될 때 방화벽체계를 보장할수 있는가를 결정한다.
- 비상대책안을 점검한다.
- 비상대책안, 문건을 작성한다.

Information Security Policies and Precedures (Thomas Peltier, Auerbach Publications)는 정보보안방책을 처음으로 개시하는데서 큰 도움이 될수 있는 참고서이다. 포괄적인 보안방책이 없으면 이 도서는 만병통치약으로 될수 없다. 그러나 이 도서는 수많은 계획들과 대책안들이 수렁창에 빠지지 않고도 보안방책을 신속히 전개해 나가는데 도움을 준다.

이러한 분석과 조사는 반드시 기관의 기업적목적의 테두리안에서 진행되여야 한다는 것은 명백하다. 정보체계보안이 위험관리에 관한 문제이지만 회사의 기업전략의 틀거리안에서 관철되지 않으면 그 보안은 실패하기 마련이다.

3단계: 호스트쏘프트웨어평가스캔을 진행한다.

방화벽설정이 잘되여 있지 않으면 비법적인 대상이나 외부사람들이 방화벽이 있음에도 불구하고 망으로 침입해 들어 올 가능성이 있다. 개별적인 방화벽호스트에 대한 쏘프트웨어스캔을 수행함으로써 구체적인 취약점들을 발견해 낼수 있다. 이 스캔도구들은 보안상 허점들을 발견하고 체계상 약점들을 구체적으로 알려 주며 방책들을 확인하고 회사의 보안전략들을 실시하게 한다. 이러한 도구들은 체계상 약점들을 검사하는데서 필수적이다. 스캔도구들이 발견할수 있는 일부 사항들은 다음과 같다.

- 조작체계의 부정확한 설정
- 보안설정 및 통과암호설정에서의 부정확성
- 완충기범람
- SANS의 10대 인터네트보안위협요소의 탐지
- FreeBSD에 영향을 주는 토막화오유
- 통과암호가 없는 NT고객구좌와 관리자구좌

일부 인기 있는 스캔도구들은 다음과 같다.

- *NAI Cybercop* (http://www.pgp.com/products/cybercop–scanner)
- *ISS Internet Scanner* (http://www.iss.net/internet_scanner/index.php)
- *SAINT* (http://www.wwdsi.com/saint)
- *Symantec* (이전에는 Axent) NetRecon (http://enterprisesecurity.symantec.com/products)
- *Netcat* (http://www.10pht.com/weld/netcat/)
- *nmap* (http://www.insecure.org/nmap/index.html)

강조해야 할것은 방화벽에 대한 호스트쏘프트웨어평가스캔을 실행하는것이 방화벽점검의 한 측면에 지나지 않는다는것이다. Cybercop 같은 도구들은 실행시키기 극히 쉽다. 그러므로 그 도구들을 실행시키기 위하여 어떤 전문봉사회사를 데려올 필요가 전혀 없다. 전문보안봉사회사를 데려올 분야는 전반적인 구성의 설계, 분석, 오유수정분야이다. 어떤 회사가 와서 이 도구들을 실행시키고 결과를 고객에게 넘겨만 준다면 이것은 자기 할바를 제대로 하지 않는것으로 된다.

이것은 결국 보안기초시설은 초기에 구성해 놓아야 한다는 점을 다시 강조하는것으로 된다. 이 구성에서는 보안, 능력, 예비, 관리와 같은 항목들을 잘 고려하여야 한다. 구성을 잘하지 못하면 체계의 재설계를 계속 반복하지 않으면 안될것이다.

4단계: Firewall–1의 설정을 점검한다.

Firewall–1이 충분한 보호 및 안전기능을 제공하지만 설정이 잘되여 있지 않는 경우 보안은 침식되고 만다. 보다 심각히 검토해 보아야 할 항목들은(순서없이) 다음과 같다.

IP보내기 IP보내기는 Control IP Forwarding으로 설정해 놓아야 한다. IP보내기는 조작체계핵심부에서 기능정지시켜야 한다. 이렇게 하면 Firewall–1이 가동하지 않는 한 IP보내기는 절대로 기능활성화되지 않는다.

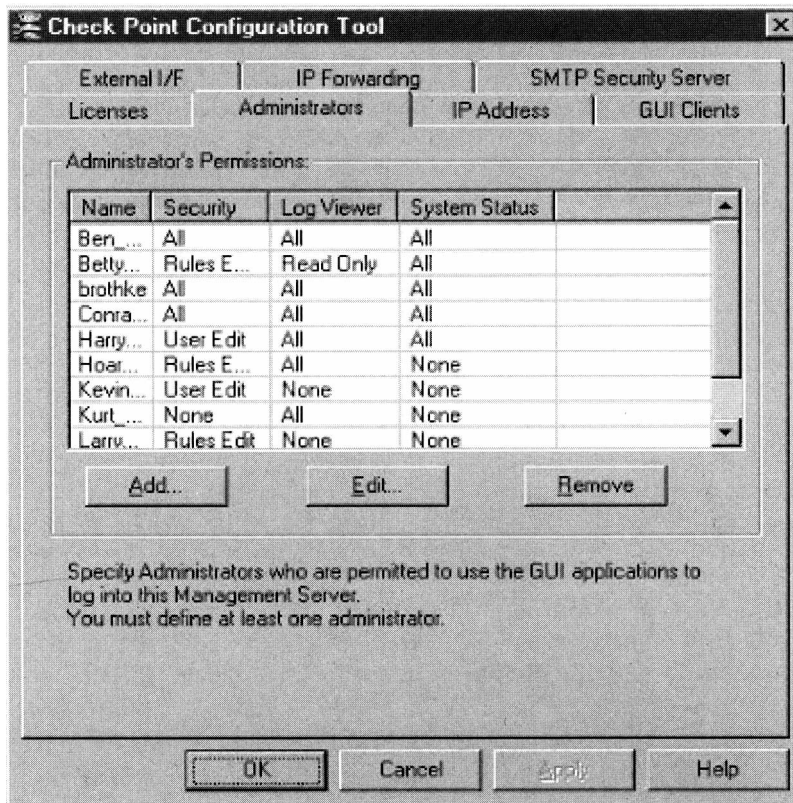



그림 10－1. 방화벽관리자들과 그 허용사항

방화벽관리자 Firewall–1관리자의 수를 꼭 필요로 하는 사람들에게만 제한되게 하여야 한다. 방화벽에 대한 매 접근의 목적(조작체계와 방화벽조작체계 두 경우)이 명백히 설명되여야 한다. 그림 10－1에는 방화벽관리자들과 그것들의 허용사항이 표로 제시되였다.

숙련된 인원 방화벽기초시설을 관리하는 인원들이 Firewall–1운명에 관한 숙련과 보안지식이 없으면 방화벽이 효력을 나타낼수 없다. 단순히 망관리경험이 있다고 하여 그 사람을 방화벽책임자로 설정해 놓으면 방화벽설정에 오유설정이 많은것으로 생각하여야 한다. 그렇게 되면 적들이 방화벽을 무너뜨리기 훨씬 더 쉽게 될것이다.

동기상태부호 SYN의 범람방지 공격자가 봉사거절(DoS)공격을 하면 먼거리의 호스트가 제대로 동작할수 없을 정도로 자원을 소모하게 된다. 동기상태부호의 범람도 봉사거절공격의 가장 대표적인 형태의 하나이다.

동기상태부호(SYN)범람방지가 적합한 수준에서 활성화되게 해야 한다. 즉 None, SYN Gateway 혹은 Passive SYN Gateway중에서 해당 항목을 선택해야 한다(그림 10－2를 볼것).

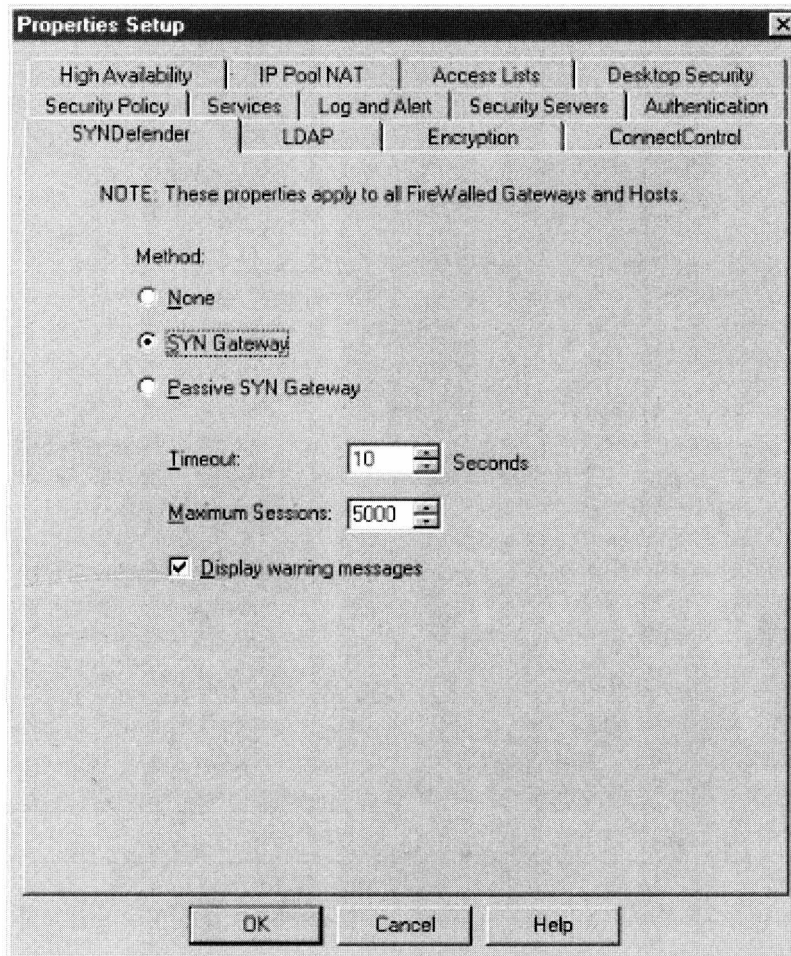



그림 10－2. 동기상태부호 SYN의 범람방지사항설정

조작체계판본조종 Checkpoint쏘프트웨어와 망조작체계를 위해서는 방화벽이 현재의 지원되는 Firewall–1판본을 실행시키게 하여야 한다. 특별히 최신판을 적재하지 않는다 하더라도 부분적재나 보강은 하도록 해야 한다.

물리적보안 방화벽은 물리적으로 안전해야 한다. 강조해야 할것은 모든 망조작체계들이 자기의 보안모형을 안전한 물리적기초시설에 근거하여 구축하여야 한다는것이다. 방화벽은 승인된 인원들에게만 접근이 한정된 구역에 배치되여야 한다.

특히

- 현지 조종반이 안전해야 한다.
- 관리조종반은 외부망에 공개되지 말아야 한다.
- 방화벽설정상태가 완전히 보호되여 손대지 못하게 되여야 한다(승인된 관리국을 제외하고).
- 현지의 관리를 맡은 관리자에 대하여 완전한 인증을 요구하게 해야 한다.
- 원격관리를 위해서도 완전인증과 암호화된 접속을 요구하게 해야 한다.

불필요한 체계구성요소들은 제거한다 콤파일러, 디바거, 보안도구를 비롯한 쏘프트웨어는 방화벽에서 제거해 버려야 한다.

충분한 예비전원공급 방화벽을 위한 UPS(무정전전원장치)가 없으면 정전되는 경우 보안이 충분히 실시될수 없다.

작업기록부검열 방화벽과 망조작체계의 작업기록부를 검열하고 분석해 볼 필요가 있다. 모든 실행과정들을 작업기록부에서 찾아 보며 그것은 디바깅과 법정분석에 리용할수 있다.

리상적으로 볼 때 작업기록부는 먼곳에 있는 작업기록부용호스트나 독립적인 디스크구역에 써넣는것이 좋다. 공격이 있는 경우에는 작업기록부에서 결정적인 문서내용을 찾아 사고의 여러 측면을 추적할수 있을것이다. 또한 이 정보를 리용하여 구멍이 난 곳들을 발견할수 있고 공격의 범위를 밝히며 또 공격에 대한 문서화된 증거를 제시하며 지어 공격의 개시점도 추적해 낼수 있게 된다. 공격자가 흔히 처음으로 하는 일은 작업기록파일들을 변경시키거나 파괴함으로써 자기의 흔적을 은폐하는것이다. 이 기록파일이 파괴되는 경우에는 예비본파일을 리용하여 사건을 추적해야 한다. 따라서 정상적으로 예비본을 해두는것은 필수적이다.

시간동기화 시간동기화의 목적은 두가지이다. 즉 시간엄수를 요하는 사건이 정확한 시간에 실행되도록 하며 서로 다른 작업기록파일들이 서로 련결되게 하는것이다. 부정확한 시간이 반영된 작업기록파일들은 가능하면 법적증거물로 제시하지 않을수 있으며 이것을 리용하여 공격자를 기소하려는 시도를 막을수 있다.

망시간규약(NTP)RFC 1305는 호스트동기화에 흔히 쓰인다. 후에 검열할수 있는 보다 높은 급의 동기화방법을 요하는 환경에서는 Certified Time (www.certifiedtime.com)에서 보내오는 시간동기제공자료들을 조사해 보는것이 좋다.

무결성검사 무결성검사는 파일체계에서 무엇이 변경되여 어느 파일에 결정적인 변화가 있을 때 그것을 체계관리자에게 통지해 주는 방법으로 되고 있다. 가장 널리 알려 지

고 리용되는 무결성검사응용프로그람은 Tripwire(www.tripwire.com)이다.

봉사와 규약의 수를 제한한다 방화벽에는 절실히 필요 없는 프로그람이 설치되거나 실행되는 일이 없어야 한다. 불필요한 규약이 있으면 불필요하게 통신련결점을 열어 놓게 된다. 포구스캔을 하여 어떤 봉사형태가 현재 열린 상태인가를 알아 낼수 있다. 봉사종류가 너무 많으면 방화벽의 효과성이 지장 받는다. 매 봉사형태를 승인 받아야 하며 승인 받지 못하는 경우에는 기능정지시켜야 한다.

위험한 구성요소나 봉사형태들은 다음과 같다.

- X 혹은 GUI관련프로그람
- NIS, NFS, RPC관련쏘프트웨어
- 콤파일러, Perl, TCL
- Web봉사기쏘프트웨어, 행정관리쏘프트웨어
- 탁상형콤퓨터용응용프로그람들(즉 Microsoft office, LotusNotes, 열람기 등)

NT용방화벽에서는 다음의 봉사형태들과 규약만 리용할수 있게 설정해야 한다.

- TCP/IP
- Firewall–1
- Protected Storage(보호보관)
- UPS (무정전전원체계)
- RPC (원격전화호출)
- Scgeduler
- Event log(사진기록부)
- Plug–and–Play
- NTLM 정보지원제공자

다른 기능들이 필요하면 요구에 따라 추가하면 된다.

조작체계를 강화시킨다 기본망조작체계에 어떤 약점이나 오설정이 있으면 firewall–1이 침식될수 있다. 방화벽은 요새처럼 보호되여 보안의 성새로 되여야 한다. 방화벽이 결코 일반용콤퓨터로 취급되여서는 안된다.

조작체계를 강화시키는 방법에 대해서는 다음의 우수한 문건들을 보면 된다.

- Amoring Solaris (www.enteract.com/~1spitz/armoring.html)
- Amoring Linux (www.enteract.com/~1spitz/linux.html)
- Amoring NT(www.enteract.com/~1spitz/nt.html)

미리 강화된 장치를 필요로 하는 사람들은 Nokia방화벽을 사용할수 있다(www.nokia/securerity sloutions/network/firewall.html). Nokia사의 방화벽은 Firewall–1을 내장한 하드웨어식이다. 방화벽의 기능을 높이기 위하여 강화되고 최량화된 IPSO조작체계상에서 실행된다.

Firewall–1의 특성 그림 10－3은 Security Policy(보안방책)표쪽을 보여 준다. 필요 없는 항목들은 표식하지 말아야 한다.

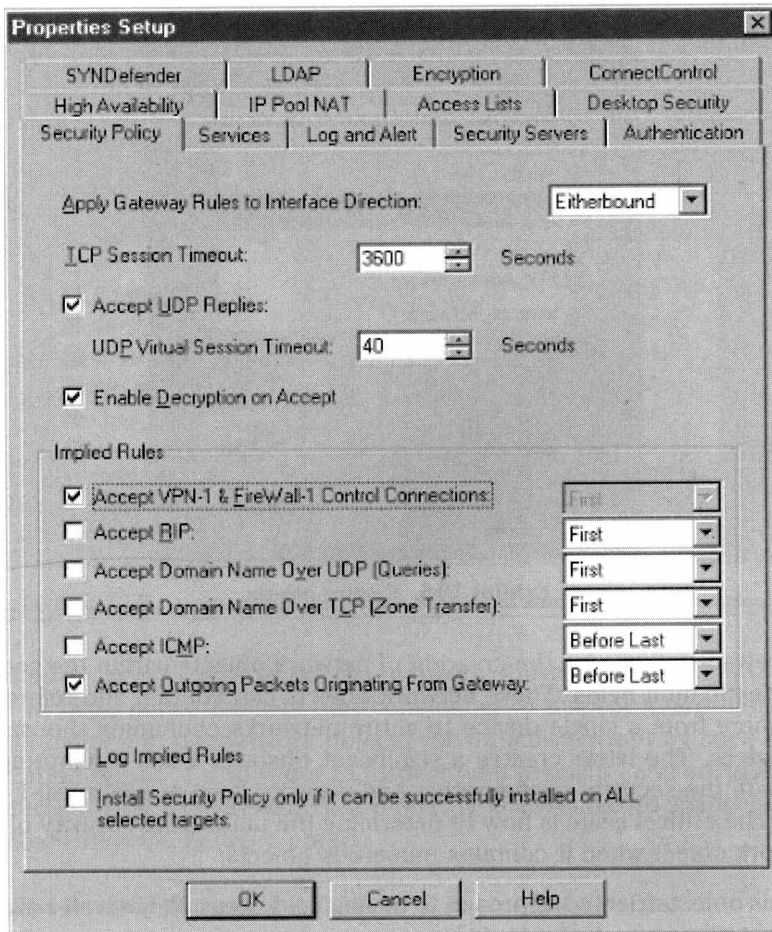



그림 10－3. 보안방책표쪽

- **ICMP** 4.0판에서는 ICMP용Checkpoint의 정상상태점검(Stateful Inspection)을 리용하기 위하여 기능활성(enable)상태는 놓아 둘 필요가 있을수 있으나 일반적으로는 이 특성을 기능정지(disable)해두는것이 좋다.
- **Zone transfer** 대부분의 싸이트에서는 DNS내리적재를 실행할수 없다. RIP와 DNS참조항목에서도 마찬가지이다.

Firewall–1의 망객체 Firewall–1에 대한 점검의 핵심적측면은 규정된 망객체전체를 분석하는것이다. Firewall–1의 망객체들이란 보안방책의 부분으로서 서로 묶어 진 론리적인 실체들을 말한다. 실례로 한 무리의 Web봉사기들은 간단한 하나의 망객체로서 거기에도 하나의 규칙이 적용된다. 모든 망객체는 망주소와 부분망디스크를 비롯한 한조의 속성을 가진다. 망객체의 부분으로 될수 있는 실체들은 대표적으로 다음과 같다.

- 망과 부분망
- 봉사기
- 경로기
- 교환기
- 호스트들과 관문
- 인터네트령역
- 우의것들의 모임

Firewall–1은 송신지와 수신지사이의 망객체들을 형성할수 있게 한다. 이 망객체들은 단 한개의 기구로부터 수천개의 기구들을 포함하는 망전체까지 포함하여 참조할수 있다. Firewall–1방화벽의 보안설정형태와 보안수준을 평가하려고 할 때 이 망전체는 상당한 난관을 조성하게 된다. 심각한 문제점은 망객체가 수많은 객체들을 포괄할 때 자기의 기본안전상태를 어떻게 결정하는가 하는것이다.

Firewall–1에서 기구들에 대하여 이렇게 객체지향적인 수법으로 관리하게 되면 방화벽관리자는 경로기나 기타 다른 기구들을 망객체로 규정할수 있게 되며 방화벽보안방책의 규정내에서 이 객체들을 사용할수 있게 된다. 망객체들은 많은 수의 망기구들을 참조하는데서 능률성을 보장하기 위하여 주로 사용된다. 이렇게 되면 호스트이름, IP주소, 위치 등과 같은것들을 기억할 필요가 없게 된다. 이러한 객체들을 리용하면 망객체들의 사용상 편리와 시간절약이 상당한 수준으로 높아 지지만 각 기관에서는 그 객체에 소속되여 있는 모든 기구나 장치들이 정말로 신뢰성이 있는가에 대하여 검토해 볼 필요가 있다. 그림 10－4에는 일부 현존객체들을 담은 Network objects창문이 있다. 그림 10－5는 망객체에 소속된 수많은 워크스테이션들을 보여 주고 있다.

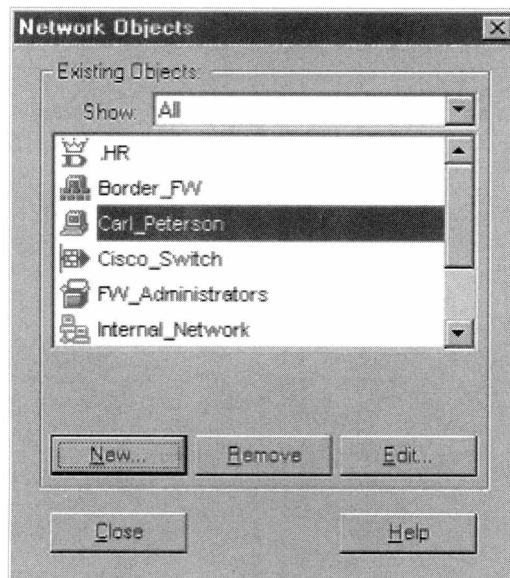



그림 10－4. 현존 객체들

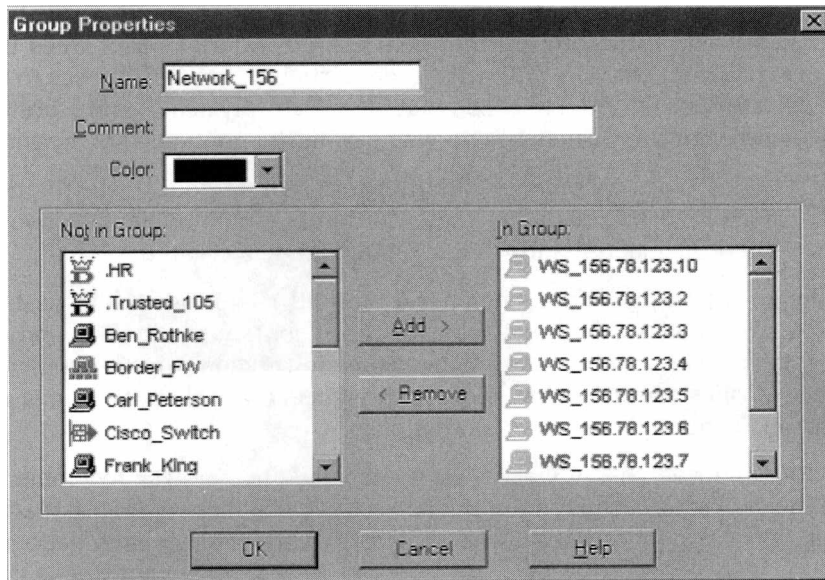



그림 10－5. 많은 워크스테이션들을 하나로 묶은 망객체

우에서 언급되였지만 망객체를 이렇게 사용하는것은 관리자의 견지에서 볼 때에는 시간이 절약되는것으로 되나 보안상 견지에서는 문제성이 있다. 그것은 망객체에 포함되는 모든 실체에 대하여 자동적으로 《내장형신뢰》가 구성되기때문이다. 이것은 대형망들에서는 망객체에서 정의된 매 개별적인 실체들을 하나하나 조사하는것이 시간이 많이 든다는 사정과 관련된다. 이러한 설정에 의한 애로가 있으므로 방화벽규칙이 제공하는 보호상태를 정확히, 정밀하게 검사하기 위해서는 망객체안에 있는 모든 장치들을 남김없이 검사하는것이 필수적이다.

5단계: Firewall-1의 규칙기지를 점검한다

규칙기지를 점검하는 목적은 이 방화벽이 어떤 봉사형태와 자료들을 허용하는가를 알자는것이다. 규칙기지를 분석하는 목적은 또한 불필요하거나 반복되거나 승인되지 않은 규칙들을 밝혀 내는데도 있다. 규칙들의 수를 줄이는 한가지 방도는 규칙들을 합치는것이다. 일부 경우 반복적인 규칙들은 통합시킬수 있기때문이다.

규칙기지점검의 사명은 방화벽이 규정된대로 자기의 기능을 수행하도록 하는것이다. 란스 스피츠너는 《Building Your Firewall Rule Base》에서 《공고한 규칙기지구축은 방화벽을 성과적으로 안전하게 운영하는데서 사활적인 단계이다. 어떤 가동환경과 응용프로그람들이 가장 훌륭한 방화벽으로 되는가에 대해서는 보안관리자들과 보안전문가들속에서 론의가 분분하다. 그러나 이 모든것은 방화벽규칙기지가 오설정되면 다 무의미해 진다.》라고 쓰고 있다.

규칙기지는 Checkpoint방화벽의 생명이다. 규칙기지는 방화벽에 보관된 하나의 파일로서 순서화된 한조의 규칙을 가지고 있으므로 매 방화벽에 해당한 보안방책을 규제해준다. 규칙기지에 대한 접근은 방화벽을 직접 관리하는 사람들에게 혹은 설정할 때 규제

된 GUI의뢰기명단에 있는 한 성원에게만 제한되여 있다.

하나의 규칙은 원천지와 목적지, 봉사형태의 측면에서의 통신을 해석한다. 규칙은 또한 통신을 허용하겠는가 허용하지 않겠는가 그리고 사용 및 작업기록부에 기록할것인가 하지 않을것인가를 규정해 준다.

Firewall–1의 검사엔진은 《최적합》(best–fit)에 대치되는 개념인 《초적합(first–fit)》도구이다. 즉 20개의 규칙을 가진 규칙기지가 있는데 들어 오는 파케트가 규칙 4번에 일치한다고 하면 검사엔진은 즉시에 멈춰 서서(규칙을 매 파케트별로 순서 있게 찾아 보게 되므로) 규칙기지의 나머지 부분은 커지지 않는다는것이다.

규칙기지점검에 대하여 보안전문가인 란스 스피츠너는 그 목적은 규칙이 30개를 넘지 않게 하는것이라고 권고하였다. 30가지이상의 규칙이 있으면 복잡성은 기하급수적으로 늘어 나 오유가 생기게 된다.

매 규칙기지는 독립적인 하나의 이름을 가진다. 공통적인 명명관례에 따라 표준화하는것이 유용하다. 좋기는 《방화벽이름–관리자이름의 첫 글자–변경날자》식으로 하는것이 좋다(례:ful–am–071201).

이러한 명명관례를 따르면 방화벽관리자가 그 규칙기지가 어느 방화벽에 소속되여 있는가, 그 규칙기지가 마지막으로 언제 변경되였는가, 누가 현 설정으로 마지막변경을 하였는가를 정확히 알수 있게 한다. 규칙기지점검을 위해서는 개개의 규칙을 검열해야 한다.

여섯가지 규칙을 가진 간단한 규칙까지의 례(그림 10－6에서 보여 줌)를 다음과 같이 볼수 있다.

- **규칙** 1**과** 2는 GUI에서 승인되여 있는 관리자들이외에는 누구도 방화벽에 직접 접근할수 없다는 비밀화규칙이라는 개념을 시행한다. 규칙 1은 해당 관리자그룹성원이 아닌 사람이 보내는 파케트이면 어떤 파케트이건 Firewall–1이 버리게 한다. Firewall–1의 봉사는 미리 지적되여 있고 또 모든 Firewall–1관리포구들을 규제하고 있다. 비밀화규칙은 패키지를 거절(reject)하지 않고 버리는(drop)것이다. 패키지를 거절하면 보내는 사람이 먼 이쪽에 무엇인가 있다고 생각하게 되며 버린다면 먼 이쪽에 호스트가 있다는것을 잘 모를것이다. 또한 이 규칙은 사용기록이 되므로 이 방화벽에 누가 직접접근하려고 시도하는가에 대한 구체적인 정보가 수집될수 있다.
- **규칙** 3은 임의의 호스트전자우편이 내부우편봉사기에 련결되는것을 허용한다.
- **규칙** 4는 임의의 호스트 HTTP와 HTTPS가 내부Web봉사기들에 련결되는것을 허용한다.
- **규칙** 5는 내부호스트가 4가지 규정된 규약을 위하여 인터네트에 접속하는것을 허용한다.
- **규칙** 6은 청소규칙이다. 이 시점에서 방화벽이 처리하지 않은 파케트가 있으면 버리고 기록해 둔다. 사실 이 시점에서 방화벽이 처리하지 않은 파케트들은 아무렇게나 버려도 되는것이다. 이 청소과정의 우점은 이 파케트들을 기록부에 기록한다는데 있다. 이렇게 되면 어느 파케트들을 방화벽이 처리하지 않았는가를 알수 있게 된다. 이것은 규모조절성이 보다 높은 방화벽구조를 설계하는데 도움이 될수 있다.

Security Policy - BorderFW_BR_22JAN2001 | Address Translation - BorderFW_BR_22JAN2001

No.	Source	Destination	Service	Action	Track
1	FW_Administrators	Border_FW	FireWall1	accept	Long
2	Any	Border_FW	Any	drop	Long
3	Any	Mail_Servers	smtp	accept	
4	Any	Web_Server	https http	accept	
5	Internal_Network	Any	http https gopher nntp	accept	
6	Any	Any	Any	drop	Long

그림 10－6. 단순규칙기지

우에서 본 규칙기지의 례는 여섯가지 규칙만이므로 좀 간단하다. 기업들에서 가지고 있는 대부분의 규칙기지들은 보다 구체적이며 복잡하다. 50개의 규칙과 수천개의 망객체들을 가진 하나의 규칙기지를 다 통과하는데는 한참 시간이 걸릴것이다.

그림 10－7에는 내용이 좀 더 있는 규칙기지 하나를 보여 준다.

- **규칙** 1은 비밀화규칙을 시행한다.
- **규칙** 2～4는 우편봉사기와 의뢰기사이의 우편전송을 허용한다.
- **규칙** 5는 임의의 호스트 HTTP가 내부Web봉사기에 련결되는것을 허용한다.
- **규칙** 6은 DMZ(비무장지대)와 인트라네트사이의 자료전송을 차단한다.
- **규칙** 7～8은 DMZ와 인트라네트사이에서 오가는 자료들을 다 차단한다.
- **규칙** 9는 파도량의 자료흐름을 초래하는 규약은 버리는데 이 경우에는 nbdatagram, nbname과 nbsession이 그런 자료들이다.
- **규칙** 10은 청소규칙이다.

점검과정에 그 어떤 규칙이 실지 필요 없다고 생각되면 그 규칙을 기능정지시킬수 있다. 일반적으로 어떤 규칙이 기능정지 당하였지만 의견이 제기되지 않으면 그 규칙은 삭제해 버릴수 있다. 그림 10－8은 기능정지된 규칙의 례를 보여 준다.

암시적허위규칙 허위규칙들은 정상규칙기지상에는 나타나지 않으나 Security Policy의 Properties Setup판의 설정에 기초하여 Firewall–1이 자료적으로 창조하는 규칙들을 말한다. 이 규칙들은 Security Policy대면부에서는 규칙기지와 함께 볼수 있다. 그림 10－9에는 암시적허위규칙의 례를 규칙하나를 가진 규칙기지와 함께 보여 주고 있다.

그 단 하나의 규칙이 암암리에 모든 자료송신을 다 버리지만 그래도 방화벽을 통과할수 있는 통과량(자료)은 많다. 이 암시적허위규칙들에서 보는바와 같이 대부분 련결성이 있음으로 하여 방화벽의 내부운영이 진행되는것이다.

6단계: 모든 자료를 보고서에 반영한다.

사업이 전부 끝난후 방화벽점검내용을 문건화해야 한다. 점검후 보고서를 작성하는 것은 나타난 결함들을 수정할 때 의거할수 있는 문건적기초를 마련하는것이다.

앞에서도 언급되였지만 스캔도구들이 쓰기 편리하므로 큰 보고서를 하나 작성하는것은 간단하다. 그러나 방화벽점검보고서가 의뢰자에게 가치 있는것으로 되기 위해서는 다음의것들을 포괄하여야 한다.

- 현 보안상태를 서술한다. 현 망환경과 현 보안태세의 기본상태를 구체화한다. 기관의 전반적보안목적과 일치시키기 위하여 이것을 기업위험분석에 참조적으로 붙인다.
- 모든 보안상의 허점들을 밝힌다.
- 수정안, 대책안, 시행의 우선권 등을 권고한다. 구체적인 시행안을 제기하여 모든 대책안들과 수정안들의 예상효과를 제시한다.

Security Policy - DMZ2_BR_12JAN2001 | Address Translation - DMZ2_BR_12JAN2001

No.	Source	Destination	Service	Action	Track
1	Any	Main_FW	Any	drop	Alert
2	Intranet_NY	Mail_Server	pop-3	accept	Long
3	Any	Mail_Server	smtp	accept	Long
4	Mail_Server	Any	smtp	accept	Long
5	Any	Web_Servers	http	accept	Long
6	DMZ_Net	Intranet_NY	Any	reject	Alert
7	Intranet_NY	DMZ_Net	Any	reject	Alert
8	Intranet_NY	Any	Permitted_Internet_Services	accept	Long
9	Any	Any	Chatty_Protocols	drop	
10	Any	Any	Any	drop	Alert

그림 10−7. 복합규칙기지

그림 10−8. 기능정지된 기지

Security Policy - Empty rule base | Address Translation - Empty rule base

No.	Source	Destination	Service	Action	Track	Install On	Time	Comment
-	FW1 Host	FW1 Host	FW1	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	FW1 Host	FW1_log	accept		Gateways	Any	Enable FW1 Control Connections
-	gui-clients	FW1 Management	FW1_mgmt	accept		Gateways	Any	Enable FW1 Control Connections
-	FloodGate-1 Host	FW1 Management	FW1_ela	accept		Gateways	Any	Enable FW1 Control Connections
-	Any	FW1 Host	FW1_topo	accept		Gateways	Any	Enable FW1 Control Connections
-	Any	FW1 Host	FW1_key	accept		Gateways	Any	Enable FW1 Control Connections
-	Any	FW1 Host	IKE	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	Any	IKE	accept		Gateways	Any	Enable FW1 Control Connections
-	Any	Any	RDP	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	CVP-Servers	FW1_cvp	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	UFP-Servers	FW1_ufp	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	Radius-Servers	RADIUS	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	Tacacs-Servers	TACACS	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	Ldap-Servers	ldap	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Host	Logical-Servers	load_agent	accept		Gateways	Any	Enable FW1 Control Connections
-	FW1 Module	Any	Any	accept		Gateways	Any	Enable Outgoing Packets
1	Any	Any	Any	drop		Gateways	Any	

그림 10－9. 암시적허위규칙

● 원가, 사용상 편의, 업무요구사항들 그리고 허용수준의 위험요소들과 관련한 보안대책안에 대한 구체적인 분석을 한다.
● 앞으로의 참고와 비교를 위한 기초자료를 제공하여 체계가 안전하게 가동하기 시작하도록 한다.

결 론

방화벽의 효과는 그것을 얼마나 정확히 시행시키는가 하는데 달려 있다. 게다가 오늘의 기업환경에서는 방화벽의 설정이 잘못되기 쉽다. 방화벽설치를 점검함으로써 방화벽관리자들은 방화벽이 제대로, 예견한대로 통제수단으로서의 작용을 하도록 하여야 한다. 이렇게 하면 기분도 좋아 지고 보안상태도 좋아 질것이다.

참 고 문 헌

1. Checkpoint Knowledge Base, http://support.checkpoint.com/public/.
2. Checkpoint resource library, http://cgi.us.checkpoint.com/rl/resourcelib.asp.
3. Phoneboy, www.phoneboy.com, Excellent Firewall-1 resource with large amounts of technical information.
4. Auditing Your Firewall Setup, Lance Spitzner, www.enteract.com/~lspitz/audit.html, www.csiannual.com/pdf/f7f8.pdf.
5. Building Your Firewall Rule Base, Lance Spitzner, www.enteract.com/~lspitz.
6. Firewall-1 discussion threads, http://msgs.securepoint.com/fw1/.
7. SecurityPortal, www.securityportal.com; latest and greatest firewall products and security news.
8. Marcus Ranum, Publications, Rants, Presentations & Code.
9. Pragmatic security information, http://web.ranum.com/pubs/index.shtml.
10. Internet Firewalls Frequently Asked Questions, www.interhack.net/pubs/fwfaq/.
11. SecurityFocus.com, www.securityfocus.com.
12. ICSA Firewall-1 Lab Report, www.icsa.net/html/communities/firewalls/certification/vendors/ checkpoint/firewall1/nt/30a_report.shtml.
13. WebTrends Firewall Suite, www.webtrends.com/products/firewall/default.htm.
14. Intrusion Detection for FW-1, http://www.enteract.com/~lspitz.

보충참고문헌

1. Zwicky, Elizabeth, *Building Internet Firewalls,* O'Reilly & Assoc., 2000, ISBN: 1565928717.
2. Cheswick, William and S. Bellovin, Firewalls and Internet Security, Addison Wesley, 2001, ISBN: 020163466X.
3. Garfinkel, Simson and G. Spafford, Practical UNIX and Internet Security, O'Reilly & Associates, 1996, ISBN 1-56592-148-8.
4. Norberg, Stefan, *Securing Windows NT/2000 Server,* O'Reilly & Associates, 2001, ISBN 1-56592-768-0.
5. Scambray, Joel, S. McClure, and G. Kurtz, *Hacking Exposed: Network Security Secrets and Solutions,* McGraw-Hill, 2000, ISBN: 0072127481.

참고싸이트

1. CERT/CC Advisories, www.cert.org/contact_cert/certmaillist.html.
2. @stake, http://www.atstake.com/research/advisories/index.html.
3. CIAC, http://ciac.llnl.gov/.
4. Firewall-1 mailing list, www.checkpoint.com/services/mailing.html.
5. Firewalls mailing List, http://lists.gnac.net/firewalls/.
6. Firewall Wizards List, www.nfr.com/forum/firewall-wizards.html.
7. CERIAS, www.cerias.purdue.edu/.
8. Bugtraq, Bugtraq-request@fc.net.
9. NTBugtraq, Ntbugtraq-request@fc.net.
10. ISS X-Force Advisories, www.iss.net/mailinglist.php.
11. Sun, www.sun.com/security/siteindex.html.
12. Microsoft, www.microsoft.com/security.
13. SANS, www.sans.org.

제１１장. 방화벽기술비교

퍼 토쉐임

2001년 1월 초에 새로운 Web페지가 개설되였다. 이름은 Netscan으로 달았다. 이 페지의 창설자들은 자기들의 Web페지를 개설하느라고 많은 수고를 하지 않으면 안되였다. 사실 그 일은 간단하면서도 시간이 많이 드는 일이였다는것이다. 그들은 경로조정된 전체 IPv4주소공간을 ping지령으로 접속확인하였다. 즉 더 정확히 말하여 .0 혹은 .255로 끝나는 모든 IP주소들을 다 조사해 보았다. 매개 ping지령에 대하여 하나의 ping중계를 기대하였다. 하나이상의 파케트로 대답하는 매개 망에 대하여 그들은 응답수를 계산하고 그 결과를 자료기지에 기록하였다. 보낸 매개 파케트에 대하여 하나이상의 파케트로 대답하는 모든 망들은 증폭기망으로 된다고 보았다. 그들은 전체 인터네트(많건 적건)를 ping지령으로 접속확인해 본후 Web싸이트에 1,024개의 가장 락후한 망들의 명단을 공개하였는데 거기에는 해당 IP주소와 그 주소에 해당한 사람의 전자우편주소와 그와 관련한 망이 올라 있었다. 가장 락후한 망들이란 단일 ping지령에 대하여 가장 높은 수자의 대답을 보내온 즉 증폭효과가 가장 큰 망들을 의미하였다.

여기서 보안문제는 원천 IP주소를 위장하여 망으로 ping요구를 보내기가 상당히 쉽다는것이다. 그리고 수신망이 응답할 때에도 초기 ping지령이 출발한 원천지주소로 모든 응답들이 오게 된다. 그림 11－1에서 보여 주는바와 같이 공격자들은 이 공정을 련속반복하여 최종 수신자의 인터네트접속에 범람을 일으킬수 있다.

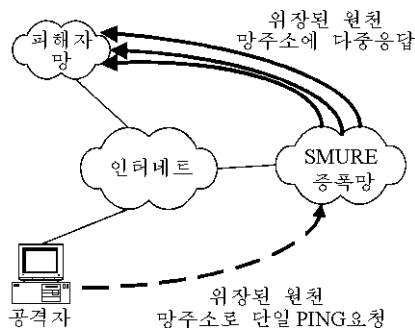



그림 11－1. 공격자가 취약한 중간망을 통하여 위장된 PING파케트들을 망에 범람시키는 수법

사실상 공격자들은 ISDN접속을 리용하여 T3(45Mbit)접속을 방해할수 있는 충분한 전송량을 마련한 다음 여러개의 SMURF증폭기망을 통하여 공격을 개시한다. 이러한 증폭을 허용하는 망이 있는 이상 그 망자체가 증폭문제를 가지고 있지 않다 해도 공격대상으로 될수 있다. 또한 이러한 공격을 미리 막는데는 방화벽만한 보안체계는 없다.

이러한 형태의 공격이 여러번 계속 진행되여 2000년 2월에 인터네트의 일부 인기싸

이트들인 Yahoo, CNN, eBay와 Amazon등이 공격을 받게 되였다.

오늘 SMURF증폭기망을 검색하여 그 결과를 공개적으로 발표하는 Web싸이트들은 여러개가 있다. 저자는 2001년 3월 어느 한 회의에서 이러한 증폭기로 사용되지 않으면 안되는 망들의 수는 2001년 1월까지 1,000배이상으로 증가하였다고 강조하였다.

이 공격들에서 찾은 흥미 있는 자료의 하나는 이 문제의 책임이 방화벽에 있는것이 아니라 경로기에 있다는것이다. 그것은 정확하였다. 이러한 경우들에서는 설정이 잘못된 인터네트경로기들이 문제의 기본요인이였다. 더우기 문제로 된것은 ping형식의 이러한 특정공격을 막기 위한 유일한 방도라는것이 망들을 인터네트에 련결시키는 모든 경로기들에서 하나의 파라메터를 설정하는것이였다. 이것이 현재 RFC 2644/BCP34(경로기의 방향조정방송의 기존값변경)에서 권고되는 기존값으로 되였다. 보안전문가들은 또한 RFC 2827/BCP 0038(망진입려과: IP원천주소위장을 리용한 봉사거부공격을 좌절시키는 방도)이라는 항목도 읽어 위장형공격에 대한 리해를 심화시켜야 할것이다.

이러한 공격이 있은후 또하나의 흥미 있는 현상은 일부 보안전문두뇌들의 조언을 받아 대통령이 《전국정보체계보호계획》을 발표한것이다. 본 저자의 견해에는 이것이 누가 제일 웃단위에서 보안을 보며 누가 보안을 책임져야 하는가에 대한 확고한 실례로 된다고 본다. 즉 회사의 리사회와 최고경영자가 책임져야 한다는것이다.

CNN, Yahoo, Amazon과 같은 Web싸이트들은 모두 방화벽들을 가지고 있으나 이 공격들을 막지 못하였다. 따라서 방화벽기술들에는 어떤것이 있으며 그것들은 어떤 보안을 제공하는가에 대하여 토론할 여지가 있다.

방화벽기술에 대한 설명

《인터네트방화벽빈도질문대답란》에는 방화벽을 두가지 부류로 가를수 있다. 즉 망층방화벽과 응용층방화벽(응용대리방화벽 혹은 대리라고도 부른다.)의 두가지가 있다. 이 장에서는 정상상태검열방화벽들을 망층방화벽과 응용층방화벽의 혼용으로 정의하였다. 그 목적은 둘사이의 류사성과 차이점을 쉽게 리해하기 위해서이다.

응용프로그람층
표현층
대화층
전송층
망층
자료련결층
물리층

그림 11－2. OSI 7층모형

독자들은 이미 OSI층모형에 익숙하여 망층은 제3층이고 응용층은 제7층이라는것을 그림 11－2에서 볼수 있을것이다.

방화벽은 일종의 보안려과장치가 있으며 둘이상의 망사이에 파케트들을 주고받는 경로기로 간단히 묘사될수 있다.

망층방화벽은 파케트려과장치

종종 파케트려과방화벽은 접근명단을 가진 경로기로 되기도 한다. 가장 기초적인 형태로서 파케트려과방화벽들은 매 IP파케트의 원천 IP주소와 목적지 IP주소 그리고 목적지포구에 기초하여 전송자료들을 조종한다. 또한 파케트려과방화벽은 들어 오는 대면부(이것이 인터네트에서 오는것인가 아니면 내부망에서 오는것인가)에 기초하여 파케트검사도 한다. 또한 원천포구, 날자와 시간, 규약형태(TCP, UDP, ICMP)와 기타 IP선택사항에 따라 또 제품에 따라 IP파케트조종도 할수 있다.

파케트려과방화벽에 대하여 잊지 말아야 할것은 우선 자체로 매개 IP파케트를 검사하지만 IP파케트들은 한 대화의 부분으로 보지 못한다는것이다. 또한 알아야 할것은 기존값으로 볼 때 많은 파케트려과방화벽들은 고장열림식설정값을 가지고 있다는것 즉 통과시키지 말라는 지령이 없는 한 파케트들을 통과시킨다는것이다. 마지막으로 또한 파케트의 HEADER부분만 검열하고는 DATA부분은 검사하지 않는다는것이다. 이것은 한 봉사안에서 다른 봉사를 턴넬화하는것과 같은 기법들은 쉽게 파케트려과를 우회할수 있다는것을 의미한다(표준Telnet포구 23이 닫겼을 때 방화벽을 통해 포구 80으로 Telnet를 가동시키나 HTTP포구 80은 열려 있다. 파케트려과장치는 원천/목적지와 포구번호를 보기만 하기때문에 그것으로 하여 그것은 통과한다.).

왜 파케트려과방화벽을 리용하는가 일부 보안관리자들은 이것을 느낄수 있는데 그들의 망에는 파케트려과를 할수 있는 많은 장치들이 있을수 있다. 가장 좋은 실례는 여러가지 경로기들이다. 대부분의(다는 아니지만) 경로기들은 오늘 접근명단을 가지고 있으므로 자기를 통과하는 IP전송을 여러가지 정도의 보안으로 조종할수 있다. 많은 망들에서는 이것을 파케트려과방화벽으로 되게끔 설정만 해놓으면 되는 문제에 지나지 않는다. 사실 모든 경로기들에 최소한의 접근목록을 장비시켜야 한다고 권고하고 싶다. 그것은 경로기자체의 보안을 위해서도 좋고 주변장치들의 최소한의 보안을 위해서도 좋다. 파케트려과는 흔히 처리률에 영향이 없거나 매우 적다. 이것이 다른 기술에 비하여 또하나의 리로운 점이다. 마지막으로 파케트려과방화벽들은 거의 모든(모두는 아니지만) TCP/IP형봉사를 지원한다.

왜 파케트려과방화벽을 리용하지 않는가 말하자면 그 방화벽들은 OSI의 3계층에서 즉 이름그대로 망계층에서 작용한다. 파케트려과방화벽은 단일IP파케트들을 검사만 한다. 그 파케트들이 하나의 대화의 일부인지는 상관하지 않는다. 특히 기본머리부정보(원천 및 목적IP주소들과 같은)만 일 없으면 파케트내용은 하나도 검사하지 않는다. 그러므로 파케트려과방화벽을 위한 그 어떤 규칙들을 만들어 내는것은 거의 불가능하고 어려우며 많은 여러 종류의 파케트려과방화벽들사이에 일관한 규칙들을 유지한다는것은 더욱 어려운것으로 보인다. 이미 언급하였지만 대부분의 경우 사고가 생기기 쉬운 기존값들은 위험한

것으로 보아야 할것이다.

정상상태검사방화벽

기본적으로 정상상태검사방화벽은 파케트려과방화벽과 같다. 그러나 파케트려과기능이외에도 접속상태를 계속 감시하는 능력이 더 있다. 대화가 시작되였는가, 현재자료전송(오든 가든)이 진행되고 있는가 아니면 종결되였는가를 동적으로 감시하는 방법으로 방화벽은 자료전송에 더욱 강력한 보안을 적용할수 있다. 또한 정상상태검사방화벽은 HTTP, FTP, SMTP와 같은 평판이 좋은 봉사도 한다. 이 마지막선택항목(이에 관해서는 제품별로 여러가지가 있다.)들을 리용하면 전송흐름을 《분석》하여 망상의 호스트의 TCP포구 80으로 HTTP전송흐름이 가는가 가지 않는가를 실지로 검사할수 있게 된다. 이때 호스트체계의 TCP포구 80으로 가고 있으므로 파케트려과장치는 이것이 HTTP전송흐름이라고 단정할뿐이다. 정상상태검사가 부분적으로 진행되므로 파케트의 자료부분을 실지 검사할 방도가 없는것이다.

정상상태검사방화벽은 대화의 개시, 통신, 종결을 리해하는 능력을 가지고 있다. 정상상태검사방화벽은 고장닫김식기존설정값을 가지고 있다. 그것은 이 방화벽이 파케트들을 어떻게 처리해야 되는지 모르면 그 파케트를 통과시키지 않는다는것을 의미한다. 이외에도 이 방화벽들은 파케트려과기에 비해 볼 때 파케트와 대화안의 실지내용(자료자체)을 《리해》함으로써 추가적인 보안수준을 보장할수도 있다. 이 마지막의것은 특정한 봉사에서만 적용되는데 제품별로 다를수 있다.

왜 정상상태검사방화벽을 리용하는가 정상상태검사방화벽들은 성능이 높으며 파케트려과방화벽보다 더 많은 보안기능들을 가지고 있다. 이러한 보안특성들을 가지고 일반봉사와 인기봉사를 특별히 조종할수 있게 된다. 정상상태검사방화벽은 파케트려과장치와 마찬가지로 거의 모든(전부는 아니고) 봉사들을 투명하게 지원한다. 그러므로 의뢰기설정을 변경시키거나 보충적인 쏘프트웨어를 추가하여 이 방화벽을 가동시킬 필요는 없다.

왜 정상상태검사방화벽을 리용하지 않는가 정상상태검사방화벽들은 응용프로그람준위의 방화벽과 같은 보안수준을 제공하지 못할수도 있다. 이 방화벽은 파케트려과장치와 마찬가지로 봉사기와 의뢰기가 서로 《직접》 대화하게 한다. 만약 방화벽이 자기를 통과하는 파케트들의 자료부내용을 어떻게 해석할지 모르는 경우에는 이것이 큰 보안위험으로 될수 있다. 특히 불안케 하는것은 많은 사람들이 응용준위방화벽에 비해 볼 때 이 정상상태검사방화벽을 틀리게 설정조작하기 쉬운것으로 잘못 생각하고 있는데 있다. 그것은 파케트려과장치와 정상상태검사방화벽이 거의 모든(모두가 아니라) 봉사들을 투명하게 지원하는 반면에 봉사준위방화벽은 제한된 수의 봉사만 지원하며 비지원성봉사와 작업하기 위하여 의뢰기쏘프트웨어에 대한 변경을 요구하는것과 관련된다.

Netcook Associates에서 발표한 백서에서 Computer Security Institute는 다음과 같이 말하였다. 《위험한 봉사형태들이 방화벽을 통과하게끔 정상상태검사방화벽들을 설정하는것은 가능할뿐아니라 사실 사소한것이다. …응용대리방화벽들은 설계상 설정오유가 나기 매우 힘들게 되여 있다.》

물론 설정이 정확히 되지 않으면 어느 체계도 안전하지 못하다는것은 너무나도 응당

하다.

사실 사람의 실수와 착오가 보안문제의 첫번째, 두번째, 세번째 리유이다. 맞지요?

응용프로그람준위방화벽

응용프로그람준위방화벽(즉 대리자)은 《중간다리》의 역할을 하는데 여기서는 의뢰기가 대리자에게 자기를 대신하여 그 어떤 과제를 수행할것을 요구한다. 이러한 과제들로서는 Web페지가져오기, 우편보내기, FTP를 리용하여 파일을 복원하기 등의 과제들이다. 대리자들은 응용에 따라 다르다. 즉 사용될 특정한 용도(즉 더 정확히 보면 응용프로그람준위 규약)를 지원한다는 뜻이다. 일반적인 대리자기능들에도 표준이 있는데 가장 인기 있는것은 COCKS이다. COCKS는 원래 데이비드코블라스가 기안하여 작성하고 NEC사가 더욱 발전시킨것이다. COCKS를 지원하는 응용프로그람들은 역시 COCKS표준을 지원하는 방화벽들을 통과할수 있게 될것이다.

정상상태검사방화벽과 류사하게 응용준위방화벽의 일반기존값들은 고장닫김식 즉 어떻게 처리해야 할지 모르는 파케트나 대화들은 다 닫아 버리게 되여 있다.

왜 응용프로그람준위방화벽을 리용하는가 우선 방화벽들은 일차적으로 매우 제한된 수의 봉사만 지원한다는 단순한 사실에 기초하여 높은 수준의 보안을 제공한다. 그러나 응용준위방화벽은 모든(모두가 아니고) 보통 봉사들을 일상적으로 지원한다. 그것들은 응용층에서의 규약을 리해하며 그렇기때문에 규약의 일부를 막아 버릴수 있다(FTP를 리용하여 파일을 접수하게 하나 FTP를 실례로 하여 파일받기를 부정하기도 한다.). 방화벽은 또한 방화벽판매업체와 방화벽판본에 따라 취약점들을 탐지하고 막아 치울수 있다.

또한 의뢰기와 봉사기사이에는 직접적인 접촉이 진행되는것이 없다. 그러나 방화벽은 의뢰기와 봉사기에 대한 모든 요구와 응답을 다 처리할것이다. 대리자(proxy)봉사기인 경우 사용자인증도 쉬우므로 많은 보안실천자들은 응용준위방화벽들에서 진행되는 많은 기록들이 얼마나 도움이 되는가를 알아야 할것이다.

성능상 리유로 하여 많은 응용준위방화벽들은 또한 자료를 완충하여 더 빠른 반응시간과 더 높은 처리률을 제공함으로써 가령 흔히 접속되는 Web페지에 접속하게 할수 있다. 필자는 방화벽이 이런 작업을 하는것을 권고하지 않는바 그것은 방화벽이 전송흐름의 검사를 진행하여 더 높은 보안상태를 유지해야 하기때문이다. 대신 보안실천자들은 일반Web싸이트접속시 성능향상을 위하여 자립형캐쉬대리자봉사기를 리용하는것을 고려해 보아야 할것이다. 이러한 자립형캐쉬대리자봉사기에 보충적인 내용보안을 마련하여 줌으로써 내용과 기타 문제에 기초하여 Web싸이트접근을 조종하게 할수 있을것이다.

왜 응용준위방화벽을 리용하지 않는가 설계상 응용준위방화벽은 제한된 수의 봉사를 지원하게 되여 있다. 다른 응용프로그람/봉사/규약을 지원하는것이 필요한 경우 응용프로그람을 바꾸어 응용준위방화벽을 뚫고 나가게 해야 한다. 방화벽과 같은 높은 수준의 보안이 주어 진 조건에서는(설정에 기초하여) 파케트려과방화벽이나 정상상태검사방화벽에 비해 볼 때 이 방화벽은 성능에 매우 부정적인 영향을 줄수 있다.

시장이 바라는것과 시장에 실지 필요한것

많은 방화벽제품들은 이러한 기술들을 서로 결합하여 간단하면서도 쓰기 쉬운것으로 만든 제품인것 같다. 방화벽들은 완성품인도방식인 《열쇠넘겨주기》혹은 《일체식》방식으로 진행되고 있다. 전원을 투입하고 켜면 설정이 다 되는 식의 방화벽보안에 대해서는 필자자신도 그닥 믿지 않고 있다. 게다가 VPN, 항비루스, 내용보안/려과, 전송자료형성 등의 류사한 기능들이 다 집적된 일체식대안도 역시 필자자신은 그닥 믿고 싶지 않다. 사실 방화벽들은 말단사용자에게 설정, 사용, 리해가 쉽게 되자면 더 복잡해야 하는것이 상례이다. 제품의 코드개수는 늘어 나며 제품의 보안취약성의 가능성도 기하급수적으로 높아 지므로 이것은 응당하다.

필자의 의견으로는 방화벽은 망에서 《검은통》으로서 대부분의 사용자들은 볼수도, 알수도 없어야 한다. 사용자들은 그것이 거기에 있다는것도 몰라야 한다.

시장은 무엇이 필요하다는것을 안다. 그렇기때문에 판매업체들은 바로 그것을 제공한다. 그러나 시장에 무엇이 필요한가를 언제나 알고 있는가. 바로 이 문제가 보안전문가들이 언제나 우선시해야 할 문제이다. 즉 보안리해와 보안의식을 가르쳐 주는것이 필요하다.

방화벽기술의 간단한 개괄

간단히 말해서 파케트려과장치는 가장 낮은 수준의 보안을 제공하나 가장 높은 처리률을 보여 준다. 보안선택사항과 특성적기능들은 제한되여 있고 망에 수많은 파케트려과장치들이 있으면 관리하기 어려울수 있다.

정상상태검사방화벽의 보안수준은 보다 높지만 파케트려과기만큼한 처리률이 나오지 못할수 있다. 판매되고 있는 주요방화벽들은 오늘 정상상태검사방화벽으로서 이것들은 대개 보안, 관리능력, 처리률, 투명한 집적도를 다방면적인 환경에 맞게 잘 결합시킨것으로 본다.

응용준위방화벽들은 보안수준은 가장 높지만 다른 두 방화벽기술들에 비해 볼 때 처리률은 대체로 그것보다 못하다.

어쨌든 보안전문가들은 절대로 방화벽자체가 보안을 잘 제공할것이라고 믿지 말아야 한다. 그리고 회사가 어떤 방화벽을 배비하였던지 관계없이 설정을 잘해 놓지 않으면 보안을 보장하지 못할것이다. 그러자면 상당한 일을 해야 할것이다.

울타리방어에 어떻게 방화벽들을 일치시키겠는가

사람들은 흔히 해커들은 《저멀리》인터네트에 있다고 생각하지 자기의 동료들중 그 누군가가 내부적이든 외부적이든 비법적인 행동을 하리라고는 전혀 생각하지 못하는것 같다. 그러나 가슴 아프게도 모든 콤퓨터관계범죄의 50%가 내부종업원들이 감행한것이

라는것을 보여 주는 통계자료가 있다.

그렇기때문에 방화벽보안과 그 주변환경의 작용에는 두가지가 있다고 설명할 필요가 있다. 인터네트상의 해커들이 내부망에 들어 오지 못하게 해야 하며 내부망에 있는 사람들이 외부망으로 기밀자료들을 보내지 못하게 해야 한다. 내부에 들어 오지 못하게 하는것은 쉬우나 안에서 밖으로 나가지 못하게 설정하는것은 매우 힘들다. 이러한 실례로 필자가 얼마전에 인터네트침투시험을 진행하였을 때 어떤 일이 일어 났는가를 보기로 한다.

출구려과를 못한 경우

의뢰기는 인터네트에 련결된 간단한 방화벽환경을 가진 산업의뢰기였다. 그들은 보안수준을 높이려고 외부자원들을 리용하여 자기들이 가지고 있던 인터네트경로기를 파케트려파기로 작용하게끔 설정해 놓았다. 게다가 인터네트경로기안쪽에는 정상상태검사방화벽이 있어 내부망과 련결되여 있었다. 그들은 정상상태검사방화벽의 비무장지대(DMZ)에 있는 항비루스(AV)전자우편관문과 인터네트사이에서 전자우편(SMTP, TCP포구25)만 오갈수 있게 경로기와 방화벽을 설정해 놓았었다. 항비루스전자우편관문은 들락날락하는 모든 전자우편들을 검사한후에야 내부망에 있는 사람이든 인터네트에 있는 사람이든 최종접수자에게 넘겨 주군 하였다. 경로기는 놀랄 정도로 잘 설정되여 있었다. 들어 오는 접근목록은 극도로 엄격하여 들어 오는 SMTP를 TCP포구25에만 돌려 주게 되여 있었다. 정상상태검사방화벽의 경우도 마찬가지였다.

SMTP항비루스전자우편관문에 대한 검사를 하던중 필자는 취약성을 찾기 위하여 항비루스전자우편관문의 SMTP접속구에 접속할 때마다 그 접속구도 대신 SMTP접속개시기발과 함께 Windows NetBIOS요구신호를 맞받아 보내 오는것을 갑자기 발견하게 되였다.

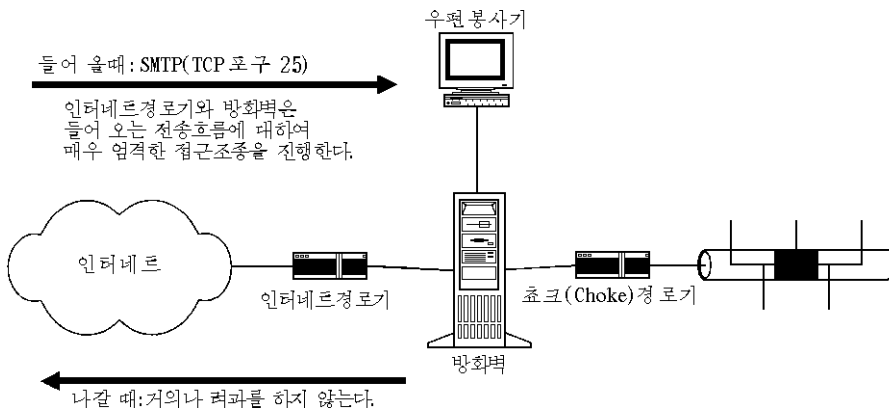



그림 11－3. 경로기와 방화벽에서 출구려과를 하지 못하는 경우

중요한 정보가 비법사용자들에게 공개될수 있다.

이 단순한 사실은 허가 받지 못한 비법적인 사람에게 많은 정보를 루설하여 준다(그림 11－3을 볼것). 첫째로, 인터네트경로기와 방화벽 두곳에서 모두 출구려과가 분명히

없다는것이다. 이것은 내부체계(최소 DMZ에 있는 이 기계)들이 외부망과 TCP/IP상에서 NetBIOS통신을 할수 있다는것을 명백히 보여 준다. 여러가지 측면에서 이것은 매우 위험하다. 둘째로, DMZ에 있는 항비루스전자우편관문에 NetBIOS가 설치되여 있는데 그것은 고도의 보안환경에 Windows봉사기설치에서 권고된 규정을 제대로 지키지 않았다는것을 보여 준다. 셋째로, 이 체계를 리용하여 DMZ나 다른 망(내부망까지 포함하여)에 쉽게 침투할 가능성이 높다는것이다. 그것은 NetBIOS가 동일한 사업그룹이나 령역에 있는 윈도우즈콤퓨터사이의 중심에서 통신에 사용되고 있기때문이다.

이것이 인터네트침투시험을 하는 과정에 필자가 대체로 느낀 점들이다. 물론 비법적인 사람이 우선 DMZ에 있는 봉사기로 뚫고 들어 가야 하지만 그것도 생각보다는 훨씬 쉽다.

어떻게 이런 정보류실을 막겠는가 보안관리자들은 외부망에 련결된 모든 방화벽과 경로기들이 정확히 설정되여 《위험하다》고 생각되는 봉사형태들과 외부망 특히 인터네트상의 호스트들에 리용되지 않게 되여 있는 봉사들을 모두 차단하게끔 해야 할것이다.

일반적으로 보안관리자들은 현지에서 리용하지 않는 봉사기들과 체계들이 그 어떤 방법으로라도 절대로 인터네트에 접속하지 못하게 해야 한다. 이렇게 되여야 보안이 상당히 높아 져 비루스나 트로이목마와 같은 적대적코드들이 외부망의 비법분자와 련계를 직접 맺지 못하여 체계의 통제권을 넘겨 주지 못할것이다.

이것은 방화벽 DMZ에 있는 체계들에도 마찬가지이다. DMZ에는 사용자인증이 전혀 없이도 외부에서 접근을 쉽게 할수 있는 체계들이 많다. 여기에서 기억해야 할 중요한것은 누가 체계접속을 초기에 시도하는가 하는것이다.

만일 외부체계가 DMZ에 있는 우편봉사기의 TCP포구 25(SMTP)로 접속을 해오면 이것이 들어 오는 전자우편이기때문에 정상이다. 만일 DMZ에 있는 우편봉사기가 외부체계의 TCP포구 25로 접속해 오면 이것도 밖으로 나가는 전자우편을 위한것이므로 역시 정상이다. 그러나 우편봉사기의 유일한 목적이 인터네트와 전자우편을 주고받는것뿐이라면 방화벽과 지어 경로기도 그에 맞게 설정되여야 한다.

관리를 쉽게 하기 위하여 많은 사람들은 인터네트에서 직접 자기 봉사기들을 판본갱신하고 있다. 일부 사람들은 지어 직접 봉사기에 틀고 앉아 그 어떤 제한이나 경계선도 없이 월드 와이드 Web을 올리훑고 내리훑고 하고 있다. 이렇게 하면 봉사기에 보안상 큰 위험으로 되며 주변환경에도 나쁜 영향이 미친다. 그것은 우선 트로이목마가 체계에 침습해 올수 있고 다음으로 봉사기들이 동일한 물리적/론리적망에 있는것외에 다른 그 어떤 공통적인것이 없음에도 불구하고 동일한 사용자이름과 통과암호를 가질수 있다는 점으로 보아 그것은 위험한 일이다.

앤쏘니 씨. 즈보랠스키 가이우스는 잡지 Phrack Magazine에 실린 자기의 글《당신이 죽은후 Cisco땅에서 해야 할 일》에서 이렇게 말하였다.

> 《나는 보안을 신뢰하지 않은지 오래다. 보안문제의 핵심은 우리가 신뢰를 신뢰하고 있는데 기인된다(켄 톰슨의 글 ＜신뢰를 신뢰하는데 대한 회고＞를 읽으라). 내가 보안을 믿는다면 그때에는 침투시험결과를 팔아 버리겠다.》

높은 보안상태와 쉬운 관리사이에 론리적관계가 있다고는 절대로 볼수 없으며 또 있을수도 없다. 보안은 어려우며 또 앞으로도 어려울것이다.

체계와 망을 침식하는 일반오유들

보안전문가들은 흔히 《망이란 외부에서 보면 딴딴하고 내부에서 보면 만문하다.》고 말하는데 필자는 이 말에 전적으로 동의한다. 항상 부딪치군 하는 약점들중 일부를 아래에 소개한다.

- 원격접근봉사기(RAS)가 내부망에 련결되면 사용자이름과 통과암호를 가지자마자 침입자들이 마치도 내부사용자처럼 그 망에 접근할수 있다.
- 접근명단과 기타 보안대책들은 WAN경로기와 망에서 실행되지 않는다. 자그마한 지역사무실들은 흔히 물리적보안수준이 낮으므로 사무실에 침습하기 더 쉬우며 전체 망에 심각한 위험을 조성할수 있다.
- 많은 봉사형태들은 기존값설치방식들이 있으므로 그것으로 하여 취약성을 가진다. 설치표준경로, 파일 및 디렉터리허용과 같은 알려 진 약점들이 있어서 누구나 다 완전한 통제권을 가질수 있게 되여 있다.
- 종업원들은 서면으로 된 통과암호방책을 지키지 않으며 통과암호방책은 사용자(실지 사람들)들을 념두에 두었지 일반체계계산부를 념두에 두고 작성하지 않는다.
- 여러 체계들에는 쓰지도 않는 여러가지 불필요한 봉사형태들이 가동하고 있다. 이러한 봉사형태들을 리용하여 해당 체계나 망전체에 대한 봉사거부공격(DoS)을 할수 있다.
- 봉사응용프로그람들에는 관리자특권이 있고 관리자들의 통과암호도 기존값에서 거의 변경되지 않고 있다. 실례로 프로그람의 사용자이름과 통과암호가 그 프로그람이름과 꼭 같은 예비본프로그람도 있고 계산부에 기존값으로 관리자특권도 있다. 인터네트에 있는 기존값사용자이름/통과암호들의 일부를 보라. 거기에는 수많은 서로 다른 체계에 기존값사용자이름과 통과암호가 수백개나 있다.
- 회사들은 인증체계를 확고히 믿고 그것을 비법접근을 막는 유일한 방패로 사용하고 있다. 많은 회사들과 사람들은 각이한 체계접근시 해커들에게 사용자이름과 통과암호가 필요조차 없다는데 대하여 모르고 있다. 몇초안에 체계전반을 장악할수 있는 그러한 취약점들이 있다는것을 모르고 있는것 같다.

일부 보안전문가들은 이러한 문제들의 대부분은 해소될수 없는 문제라는것을 깨닫게 될것이다. 또한 이 문제들을 잘 알고 전문가들은 이러한 문제들을 해결하거나 제거하기 위하여 끊임없이 노력해야 할것이다.

《침투시험을 칠 때 흔히 어떻게 우리 방화벽을 뚫고 들어 오시렵니까?》, 《당신은 이런저런것을 하면 안됩니다.》라는 질문과 통보문을 보게 된다. 무엇보다먼저 침투시험에서는 방화벽을 뚫는것이 아니라 방화벽을 에돌아 간다. 방화벽을 뚫는 그자체는 많은 기법들을 필요로 하지만 그것을 소유한 회사에는 큰 해가 없다. 둘째로, 해커들은 공격대

상회사의 규정이든 나라의 규정이든 그 어떤 규정도 준수하려 하지 않는다.

경영진의 워크스테이션들에서의 보안은 어떠한가 회사들은 흔히 인터네트련결환경과 자기의 내부봉사기들에 극도로 엄격한 보안조치를 취한다. 그러나 이 보안상태가 높은 체계들을 관리하는데 리용되고 있는 워크스테이션들을 안전하게 하는 사업은 그들이 잊고 있든지 아니면 소홀히 하고 있다. 어느 한 인터네트은행의 보안검사를 최근에 해보는 과정에 필자는 방화벽들과 침입탐지체계들, 대리자들과 그에 투하된 기타 장비들을 감명깊게 보게 되였다. 좀 더 깊이 검사해 보는 과정에 발견하게 된것은 보안성이 높은 체계에 대한 관리기를 그들의 내부망에 위치한 특정워크스테이션으로 한다는것이였다. 이 모든 워크스테이션들(망관리자들의 《소유》인)은 다소 기정값설정으로 즉 사용자이름과 통과암호, SNMP 등의 봉사형태들을 기정값으로 하여 여러가지 조작체계들을 기동시키고 있었다. 이 모든 워크스테이션들은 망상에서 평범한 사용자기계들과 막 섞여 있었다. 이 관리콤퓨터접근에는 사용자이름/통과암호이외에는 더 다른 제한조건들이 없었다. 지어 내부콤퓨터들사이에는 명명관례까지 있어서 어느 콤퓨터가 《기간체계관리용콤퓨터》로 리용되고 있는가 하는것까지 쉽게 알수 있게 되여 있었다. 이러한 워크스테이션들을 먼저 뚫고 들어 갔으므로(트로이목마, 물리적접근, 기타 방법으로) 기간체계에 접근하는데는 얼마 시간이 걸리지 않았다.

침입탐지체계와 방화벽

최근 자기들의 망에 침입검출체계(IDS)를 설치하는 회사들이 점점 더 많아 졌다. 이 분야도 실수하기 쉬운 분야이다. 우선 IDS는 해커들로부터 회사의 보안을 지켜 내지 못한다. 공격을 더 잘 탐지하여 문건에 기록할수도 있지만 많은 경우 공격을 막지는 못한다. IDS는 기록을 광범하게 하고 자동 및 수동분석을 잘하는 체계, 일정하게 파악 있는 체계라고 하는것이 좋을것이다.

얼마전에 누군가가 방화벽이 공격을 막는 식으로 자동적으로 여러가지 공격을 막거나 다른 체계들을 다시 설정할수 있는 IDS를 만들 기발한 착상을 들고 나온적이 있었다. 위장공격방법(요즘 매우 쉬운 방법으로 됨)으로 해커들은 믿음직한 제3자로부터 시작되는 허위공격을 진행하여 회사와 그 신뢰성 있는 원천(즉 제3자)사이의 통신을 모두 막아버린다. 그리하여 이러한 자동화된 체계에 대한 착상이 좋은 생각이 못된다는것을 모든 사람들이 즉시 깨닫게 되였다.

일부 IDS들은 서명형이나 일부는 변칙형들이다. 일부 IDS들은 량자를 선택할수 있게 되여 있고 호스트나 망에 기초한것도 있다. 그리고 물론 망에 배비한 IDS장치들에 대한 작업기록과 관리를 맡아 수행하는 중앙조종탁도 있다(이러한 중앙조종탁보안은 어느 정도인가).

- **문제** 1. 서명형탐지체계는 크든작든 특정한 자료형태들에 기초하여 공격을 탐지하게 된다. IDS가 아는 형태들을 우회하는 방법을 해커들이 알기때문에 요즘에는 이것을 우회하는것은 더 쉬워 지고 있다.
- **문제** 2. 대부분의 IDS들은 수신하는 체계가 보내오는 자료들에 어떻게 대응하는

지 모른다. 즉 IDS들은 공격을 보지만 공격이 성공적인것인지 아닌지 하는것은 모른다. 그렇다면 IDS가 어떻게 공격들을 분류하며 어떻게 공격의 성공성여부를 분석하겠는가.

- **문제** 3. IDS는 믿지 못할 정도로 허위경보를 내군 한다. 그렇다면 어느 경보는 진짜이고 어느 경보가 가짜인지 매번 누가 알아보겠는가. 일부 회사들은 IDS들이 너무 많은 경보신호를 내보내기때문에 체계를 조절하여 그렇게 많은 경보를 내보내지 않게 하는 조치를 자주 취하군 한다. 이것은 그들이 망체계에서 무엇인가 설정이 잘못되지 않았는지 알아 보지도 않고 탐지표적들의 일부를 꺼버림으로써 그 IDS의 기능들을 마비시킨다는것을 의미한다.
- **문제** 4. 변칙탐지는 《정상적인》전송흐름들에 의거하여 정상패턴과 맞지 않은 모든 비정상활동들에 대하여 경보신호를 발생한다. 그러면 어떤것이 《정상적》인 패턴인가. 필자는 언제인가 망에 IDS를 배비한것을 보았는데 각종 필요 없는 규약들과 봉사도 설정되여 있고 또 선을 통하여 평문인증이 통신되는것을 본적이 있었다. 《정상》틀이라는것은 거의 모든것을 다 통과시키고 결과 IDS의 변칙탐지능력을 크나작으나간에 마비시키는 틀이 되였다(요즘 사람들이 흔히 자기집 콤퓨터에 장치하는 《개인용방화벽》도 이렇다.).

IDS가 방화벽에 아주 효과적인 보충수단으로 되는것은 방화벽이 각이한 IP/TCP/UDP 머리부분정보와 원천지/목적지, 날자/시간과 같은 정보를 기록하기만 하는데 비하여 IDS가 공격내용기록을 더 잘하기때문일것이다. IDS를 리용하면 방화벽과 그 기록만 가지고 있는데 비하여 해커활동을 더 오랜기간에 걸쳐 통계를 내는것도 더 쉽다. 이러한 통계들이 있으면 회사의 체계들에 대한 해커공격이나 비법적인 접근이 있는 경우 경영진에 실태를 보여 주기 쉬울뿐아니라 그 사용자들속에서 전반적보안의식을 높이는데도 좋다.

한편 IDS는 방화벽보다 사람의 방조가 더 많이 필요하기때문에 회사는 이러한 체계에 대한 목적을 명백히 정한 다음에 구매하고 배비해야 한다. 해커들이 망에 들어 오지 못하게 하겠다는 순진한 목적만 가지고서는 안된다.

총체적권고와 결론

방화벽은 자료를 주고받는 체계와 망들뿐아니라 자기자체도 보호할수 있도록 설정되여야 한다. 사실상 방화벽은 인터네트도 《보호할수 있게》 되여야 한다. 즉 내부《해커》들이 인터네트에 련결된 다른 사람들을 공격하지 못하게 해야 한다는것을 의미한다. 경로기, 교환기, 봉사기들과 같은 망주변장치들도 체계자체뿐아니라 방화벽환경을 보호할

수 있게 설정되여야 한다.

보안전문가들은 인터네트접속을 허용하기전에 반드시 사용자인증을 사용하게 하여야 한다. 많은 경우 이렇게 되면 HTTP, FTP, Telnet 등과 같은 규약을 리용하여 인터네트상에서 비루스들과 트로이목마들이 호스트와 접촉하지 못하게 할수 있다.

필요 없는 말 같지만 회사의 망에서 인터네트를 개인용도에 사용하는것은 일반적으로 금지시켜야 한다. 물론 통제준위설정도 고려될수 있지만 본질상 사용자들이 POP3, SMTP, FTP, HTTP와 같은 규약들과 ASCII나 2진수형식으로 파일을 보낼수 있는 기타 규약들을 리용하여 내부망에서 파일들을 내보내거나 위험한 내용(비루스, 트로이목마)을 내리적재하지 못하게 하자는것이다.

마지막으로 회사보안방책에서 요구하는 보안수준에 부합되게 하자면 다른 도구들도 배치해야 한다. 필자의 경험에 의하면 설치된 모든 방화벽들의 50%이하가 전반기록을 수행하고 있으며 그 방화벽소유자들중 5%미만이 쓸만한 기록분석, 보고, 통제비슷한것을 실지로 하고 있다. 일부 사람들에게는 우의 모든것이 《우리에겐 방화벽이 있으니까 안전하지뭐》하는 태도처럼 보일것이다. 이런 태도는 어리석은것일뿐아니라 틀린것이다.

해커들이 구석구석에 숨어 있는 우리의 현 인터네트통신의 시대에는 최소한 방화벽들과 방화벽기술 그자체만으로는 믿을수가 없다. 허용된 규약들과 포구들을 통하여 자료를 찾아 《굴을 뚫는》해커들은 오늘날의 방화벽을 쉽게 우회할수 있으며 암호화기법을 리용하여 그 흔적을 숨길수도 있다. 그러나 보안관리자들은 일관적이며 전반적인 보안구조의 부분으로서의 방화벽이 아직도 회사의 망보안에서 중요한 부분이라는것을 인식하여야 할것이다.

제12장. 가상개별망의 보안

제임스 에쓰 틸러

가상개별망(VPN)이 수많은 각이한 기업분야에서 광범히 파급되고 있는것은 놀라운 일이 아니다. 수직적시장이나 무역에 관계없이 VPN은 유연성이 있으며 잘 실행되고 사용되면 투자의 효과성을 즉시에 볼수 있는것으로서 통신에서 결정적역할을 할수 있다. VPN은 지금까지 그 도입범위가 상당히 넓었으며 그 도입속도도 빠르다. 기술이 발전함에 따라 이 경향은 계속 증가할것이다. VPN이 이러한 파급력을 보이게 된것은 그 기술의 실현이 상대적으로 쉬운것으로 알려 진데 있다. 보건대 단순하며 누구고 무제한하게 리용할수 있다는 전망으로 하여 이 새로 발견된 통신형태를 미친듯이 리용하기 시작하였다. 그런데 VPN의 좋은 주요특징들만 보고 사람들은 미사려구가 들어 찬 판매광고와 제품소개에 그만 놀라서 그뒤에 숨은 모호한 보안상 기본약점은 보지 못하였다. 이 장에서는 VPN과 관련된 보안위험률과 VPN을 곧 보안이라고 보는 잘못된 인식에 대하여 집중적으로 보려고 한다.

여기에서 구체적으로 설명되는 보안상 제한성들은 VPN기술자체와는 거의 무관계하다는것을 반드시 리해하여야 한다. VPN기술에는 여러가지가 있는데 몇가지 실례로 IPSec, SSL, PPTP를 들수 있다. 요구사항과 실행의 견지에서 보아도 매개가 장점과 단점을 다 가지고 있다. 또 매개 기술이 다 보안수준이 다르므로 여러가지 조건들에 다 결합하여 쓸수도 있다. 이 장에서는 매체 및 과정으로서의 VPN의 불안전성에 대해서만 보고 기술적측면이나 기술적표준에 대해서는 보지 않기로 한다.

다루려는 문제는 VPN에 대한 평가인데 흔히 소비자들은 시장에 쓸어 드는 자질구레한 제품이나 소비자의 요구를 충족시킨다는 업계의 제품들을 보고 VPN에 대한 평가를 내리군 한다. 그런데 소비자의 수요는 끊임없이 높아 가는데 보안제고를 위한 충분한 기술의 개발은 실지 경험이 부족한것으로 하여 령상태나 다름 없다. VPN에 대하여 이야기할 때면 흔히 《보안》이라는 단어가 많이 쓰이군 하는데 이것은 VPN자체 즉 통신되고 있는 자료에 대한 보호를 의미할것이다. 그럼에도 불구하고 보안이 제일 필요한 점인 VPN이 끝나는 점에서 이 통신의 보안이 끝나고 마는것이다.

이 장의 목적은 VPN을 소개하며 그것이 최근에 인기가 대단한데 대하여 그리고 전역망과 같은 인터네트분야에서의 새로운 발전의 련관관계에 대하여 설명하는것이다. 또한 기성 원격접근대안들에서 경험한 보안과 최근에 업계에서 도입된 보안실천과의 대비를 보기로 한다. 이것은 희미하던 문제를 명백히 고찰하고 이 기술이 기관의 전반적보안태세에 어떤 큰 영향을 주는가를 토론하게 되는 중요한 기회로 될것이다. 문제는 사실 너무 방대하여 리해하기 힘들다. 《나무는 보지만 숲은 못 보는 격》이라고 할수 있다.

하나의 문제가 다른 문제로

VPN의 인기는 하루밤사이에 폭발적으로 올라 간것 같다. 회사의 매 원격근무자들을 위한 전용선을 관리하는 힘든 일을 다 그만두고 현재 있는 인터네트선을 리용하여 지난 시기에는 불가능하였던 수많은 결선을 다중화할수 있음으로 하여 VPN기술은 말그대로 폭발적으로 발전하게 되였다.

기술들을 잘 결합하면 흔히 그러하듯이 한 형태의 기술이 다른 형태의 기술에서 좋은 점을 섭취하고 그 성과에서 리익을 얻는것은 보통현상이다. 이것이 실현되여 기술적인 향상이나 선택으로, 그것들이 결합되여 또 실현되면 한 형태의 기술만으로는 달성할수 없는것이상을 달성하는 일석이조의 효과를 거둘수 있다. 이동전화는 이러한 현상의 대표적실례이다. 이동전화에서는 전자인증서, 암호화기술, 전자우편, 열람을 비롯한 여러 기술들과 혁신적성과들을 지원한다. 무선계에서는 흔히 망기술에서만 볼수 있던 기술들을 리용하여 왔는데 이 기술들은 현재 다른 환경에서 사용되고 있는것으로 하여 큰 주목을 받고 있다. 이동전화사용은 보다 확고하며 여기에 사용된 기술은 이전에 상상도 못하였던 방식으로 사용되였다. 이것을 흔히 이른바 《이기고 또 이기는》(“win–win”) 정황이라고 한다.

최근에 VPN을 보편적으로 도입하고 있는것은 통신산업에서의 두가지 기본변화 즉 전 세계적인 인터네트의 도입과 값 눅은 전역망에 의한 인터네트접근에 기인된다고 볼수 있다. 최근에 일어 난 이러한 변화들과 끊임없이 늘어 나는 이동성사용자들을 지원해야 할 필요성으로 하여 VPN기술은 인기의 절정에 올라 섰다.

이동성사용자

이동(roaming)에 대해서는 지난 시기 고정된 성원에 한하여 봉사를 제공하고 망의 정상적인 변두리밖에 대하여 꼭 같은 고정된 봉사만 제공하던 이전시기의 망으로부터의 자연적인 발전이라고 특징 지을수 있다. 아마 하루밤사이에 원격접근이 사용자들에게 가장 중요한것으로 되여 원격접근보장에 막대한 자원이 투하된듯 하다.

그림 12－1에서 보는바와 같이 초기에는 모뎀들을 모아 내부망접근을 허용하는 공통적인 장치에 련결하였으며 모뎀들과 전화선들이 련결되였다. 사용자들의 사용상 요구가 기하급수적으로 늘어 남에 따라 모뎀의 전송속도도 점차 올라가 변화가 림박해 졌다. 변화의 첫 물결은 바로 원격탁상형콤퓨터의 형태로, 일부 경우에는 전반적체계상에서 나타났다. 그림 12－2에서 구체적으로 보여 주는바와 같이 원격조종되거나 혹은 원격사용자에게 탁상형콤퓨터환경을 보내는 체계에 사용자는 전화번호판을 돌려 접속할수 있다. 두 경우에 다 원격사용자와 핵심체계사이에 필요되는 대역너비는 실지 작아 졌고 기능은 증폭되였다. Cubix, Citrix와 PC Anywhere회사들은 요구사항, 우점, 가격이 서로 다르지만 이러한 기술을 향상시키는 작용을 놀았다.

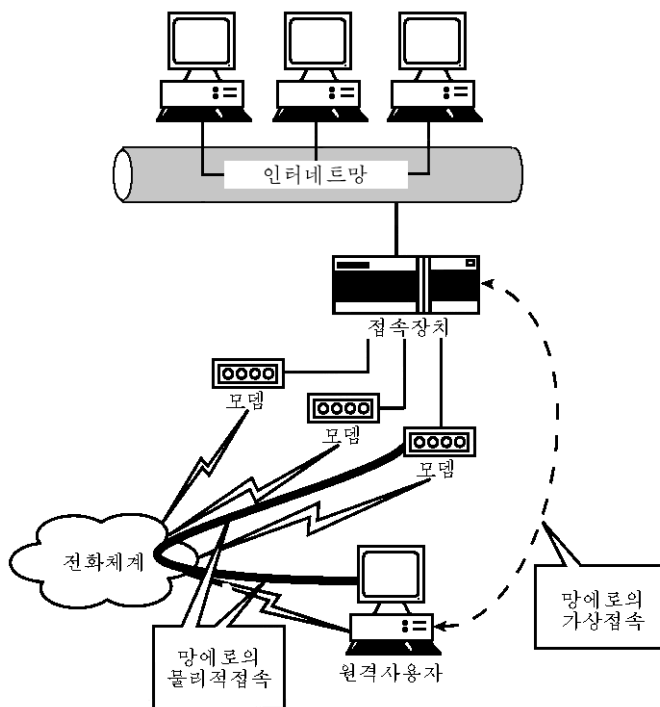



그림 12－1. 모뎀을 통한 표준원격접근

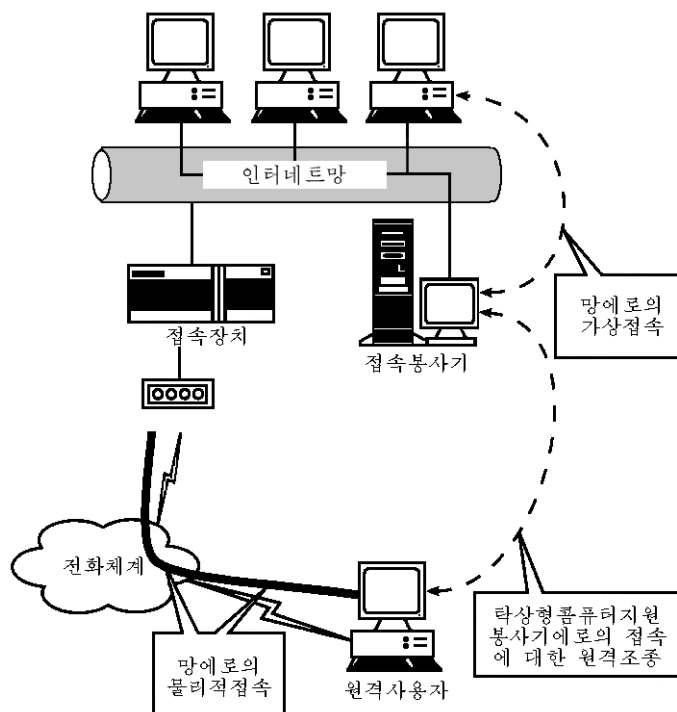



그림 12－2. 원격조종이나 원격탁상형콤퓨터를 리용한 모뎀식표준원격접근

내부망에 있는 원격접근봉사기가 다른 망자원에 매우 높은 속도로 접속하는것을 보고 성능을 판정하였다. 접근봉사기를 조종하거나 탁상형콤퓨터를 사용하는것과 같은 감각을 얻기 위하여 경량규약을 사용하니 모뎀을 통한 접속이 마치도 실지 망에서와 같은 느낌을 주었다. 원격접근이 진행되여 나가다가 내부망에서와 꼭 같은 감각을 느끼게 되면 바로 이 지점을 원격접근대안을 계측하는 기준점으로 삼았다. 이 지점에서 더 앞으로 나가면 차이가 너무 심하거나 불편한 점이 더 많이 생겨 아마 원격접근대안을 다 걸어치우고 말것이다.

인터네트리용

인터네트는 말그대로 현저한 속도로 장성하여 왔다. 통신망에 발을 처음으로 들여놓은 사람들의 수로부터 통신기술에서의 도약에 이르기까지 인터네트는 점점 더 많은 사람들이 리용하게 되여 그 밀도와 인구수는 나날이 높아 지고 있다. 인터네트는 특별한 인기라든가 단순한 흥미거리라기보다 이제는 기업과 개인통신의 필수적인 요구로 되였다. 인터네트와 련관이 없던 기업들이 지금에 와서는 이것을 발판으로 원가는 줄이면서 고객들을 더 많이 늘이고 고객들을 더잘 만족시키려고 노력하고 있다. 새 사무실이나 이미 있던 사무실이나 인터네트망을 표준설치하는것은 이제 와서 그리 드문 현상이 아니다.

반대로 전용인터네트련결선을 초기에 도입한 사람들은 대체로 회사전체에 하나의 접속점만 두었다. 그림 12－3에서 보는바와 같이 원격사무실들은 광지역망(WAN)을 지나서 중앙조종점에 이르러서야 인터네트에 접근할수 있게 된다. 인터네트의 규모와 회선수가 제한되였을 때에는 이러한 설계씨나리오가 그럴듯하였다. 인터네트접근에 대한 요구가 높아짐에 따라 인터네트가입자수는 정비례적으로 늘어 나 WAN에 과잉부하가 걸리기 시작하였다. 그로부터 얼마후 직접결선비용이 떨어 지자 인터네트는 점차 기업생활의 일부로 되여 필수적인 도구로 되였으며 그에 대한 요구는 더욱 높아졌다.

인차 인터네트는 성공하는 기업들에 있어서 필수적인 요소로 되였으며 현재 내부망들을 오가는 인터네트전송량은 놀랄 정도로 방대하다. 정보에 대한 요구는 현재 인터네트리용비보다 훨씬 더 중요하다. 과거에는 인터네트접속을 심중히 검토하고야 실행시키군 하였다. 오늘에 와서는 《얼마나 굵은 케블이 필요한가》하는 질문이 나오지 《어데에 설치하려 하는가》라는 질문은 나오지 않는다. 인터네트가 광범하게 도입되고 또 그것을 절실한것으로 받아 들임으로 하여 인터네트의 밀도와 다양성은 크게 높아 졌다. 오늘 많은 기관들에서는 접근점을 여러 곳에 가지고 그것들을 리용하여 내부망의 부하를 덜며 내부사용자들에게 더 높은 성능을 제공해 줄뿐아니라 봉사에서 여유도 조성하고 있다. 현재 있는 수많은 인터네트결선을 리용함으로써 VPN기술을 실현하여 통신을 보다 개선하면서도 VPN을 도입하기 오래전부터 수지가 맞는 봉사를 진행할수 있다.

그림 12－3. 하나의 중심점을 통한 인터네트접근과
여러개의 중심점을 통한 인터네트접근과의 비교

광 대 역

오늘 표준으로 된 인터네트에 대한 고속접속이 존재하기전에는 모뎀과 전화선만이 있어 고통스럽게 접속을 해야 하였다. 물론 그때에도 몇명 안되는 특권적인 사용자들이 있어 ISDN을 가지고 일정하게 안도감은 느끼고 있었다. 그러나 접속은 여전히 모뎀에 의한것이여서 일을 제대로 하기란 참으로 끔찍스러웠다. 원격접근의 초기도입자들은 모뎀을 가지고 자료전송과 봉사를 할수 있었다. 인터네트가 널리 퍼짐에 따라 모뎀을 인터네트접속수단을 제공하는 인터네트봉사제공자(ISP)에 련결하였다. 두 경우에 다 제한된

속도로 해서 고통은 변함이 없었다.

오늘 매 개인이 집에 앉아서 인터네트에 접속하게 되는 그 속도는 이전에 최대규모의 회사들이나 쓸수 있었던 비용이 많이 드는 선으로 이룩하였던 그 력사적인 속도라고 할수 있다. 지금은 간단한 도구를 설치하여 ISP에 접속하며 이써네트를 리용하여 집이나 자그마한 사무실에 있는 호스트콤퓨터와 접속할수 있다. 오늘 접근제공과 조종은 개인콤퓨터에서 각각 따로 진행하며 사용자가 개입할 필요가 거의 없다. 오늘 접근제공과 접근조종은 사용자콤퓨터에서 별도로 진행되며 사용자의 개입을 거의 요구하지 않는다. 사용자는 물리적련결과 통신매체의 작용에 대해서는 거의 감각하지 못한다. 사용자가 콤퓨터를 켜면 인터네트는 순간적으로 접속되여 쓸수 있게 되여 있다. 이것은 사용자콤퓨터와 모뎀이 서로 협력하여 신호종단점으로 되며 련결제공과 관련한 모든 책임을 떠맡는 물리적련결과는 상당한 대조를 이룬다.

많은 통신기술들과 마찬가지로(특히 모뎀형원격접근과 관련한) 종단점이 주어 져야 원격접근이나 모뎀을 련결할수 있다. 전화회선을 사용하는 경우 모뎀(가상모뎀이든 물리적모뎀이든)이 있어야 원격체계가 전화선으로 련결되여 통신을 할수 있게 된다. 광대역인 경우 그것이 케블모뎀기술이든 xDSL기술이든 류사한 요구가 제기된다. 즉 종단점이 주어 져야 집이나 사무실에서 원격기구가 접속을 실현할수 있게 된다.

VPN도입과 관련하여 핵심적문제인 종단점은 광대역과 모뎀을 가르는 주요 판별요인들중의 하나로 되였다. 종업원들에게 전화선에 의한 원격접근을 제공하기 위해서는 봉사기 즉 워크스테이션에 한대의 모뎀만 설치하고 전화선을 련결할수 있었다. 원격사용자에게 모뎀 한대, 전화번호 그리고 기초프로그람만 주어 지면 련결이 되여 체계와 봉사들에 충분한 접속이 이루어 지게 되였다.

반대로 광대역실현에서는 문제가 보다 복잡하고 비용은 상당히 더 들기때문에 오늘 봉사제공자들만이 이 기술을 실현하고 있다. 그 하나의 레가 바로 인터네트케블봉사이다. 케블기반에 의거하여 자기자체의 내부원격접근을 실현하는 회사들은 많지 못하다. 현재 점 대 점원격접근해결책으로는 광대역이 리용되지 않고 있다. 바로 여기에 VPN의 근본적인 매력 즉 이 선진통신기술을 리용하여 회사자원들에 접근할수 있는 방도가 있다.

속도가 상당히 증가하는것이 사람들에게 큰 호기심을 자아내는것은 바로 모뎀이 제공하는 제한된 대역너비가 사람들의 요구에 비해 보면 너무나도 좋기때문이다. 또한 콤퓨터에서 그 모뎀기술을 분리시키면 통합이 간단해 지며 규모조절도 가능해 진다. 이런 조건에서 광대역은 회사자원리용에서 극히 매력적이다. 광대역을 가지고 고속인터네트열람과 개별유람을 한다는것과 광대역기능을 가지고 기업의 목적을 위해 일한다는것은 별개의 문제이다. 그러나 우에서 언급한바와 같이 광대역기술들은 비봉사제공자기관이 내부용으로 실행하기에는 복잡하며 불가능하다. 현재 인터네트접속만 보장하는 고속통신대안은 아마 VPN의 출현전까지는 나와야 할것이다.

확 장 접 근

통신능력들이 커지고 회사들이 인터네트를 일상생활에 구현하기 위한 사업을 계속 추진시켰으므로 통신능력과 인터네트를 결합시킬수 있는 VPN기술을 창조하는것이 필수적이였다. 전화회선식인터네트접속과 광대역을 쓰면 어디에서나 고속으로 인터네트에 접속할수 있다. 두가지 다 인터네트에 전반적인 접속은 제공하지만 회사본부에로의 접속을 종단시켜 주는 가능하고도 효과적인 방도는 없다. 광대역접속은 인터네트에 가깝게 련관되고 직접전화식대안들은 비효과적이며 비용이 많이 드는것이므로 유일한 방도는 인터네트를 써서 전용통신을 보장하는것이였다. 이렇게 되여 결국 기관들에서는 자기들이 현재 가지고 있는 인터네트망에 원격련결을 다중화하게 되였다. 마지막난관은 비밀성, 정보무결성, 접근조종, 인증, 검사, 부인방지 등의 형태로 통신의 보안을 보장하는것이였다.

전 세계적인 인터네트도입은 그 사용성과 속도의 증가에 의하여 전화회선에 의한 무제한한 접근을 훨씬 릉가하게 되였다. 직렬통신자체는 전용회선으로 진행되여 해커가 침습할수 없었으며 따라서 상대적으로 안정하였다. 전화회선에 의한 망접근으로 하여 전화체계가 통신수립에 적극 활용되게 되였으며 어디 가나 전화를 통하여 인터네트를 쓸수 있게 되였다. 인터네트접속에 모뎀을 사용한다고 하면 속도는 보장되지 못하며 전화체계는 련결하느라고 계속 사용되지만 국부에서 벗어 나지 못하게 된다. 인터네트는 여전히 공통적인 련결매체로 리용되고 있다. 전화회선에 의한 원격접근만도 봉사에서 커다란 비약으로 된다. 그것은 회사들이 제공한 원격접근방식은 해외에서 접속하기 곤난한것들이기때문이다. 방책상 제한은 없었지만 전화설비와 전화계통이 오늘처럼 질이 높지 못했고 또 장거리전송으로 하여 통화가 잘 안되였기때문에 비용이 문제점으로 되였었다. 이와 반대로 세계적으로 전화번호를 보장하는 매우 큰 ISP들을 내놓고도 인터네트접속을 보장해 주는 ISP들은 수만을 헤아리고 있다. 그러다나니 접근점을 끝없이 제공해 주는것을 제외하고도 세계적인 수백개의 ISP들을 위한 료금처리와 관리를 해주는 본사로 활동하는 회사들도 있다. 사용자의 견지에서 보면 지구상에는 하나의 큰 ISP만 있는것이다.

최종적인 난관은 지난 시기 전화망으로 원격접근을 할 때 생기던것과 같은 전송과정의 영향이나 로출 등 사고로부터 통신을 보호하는것이였다. VPN기술이 바로 이 빈 공간을 메꾸어 주었다. 통신능력이 확장되고 인터네트의 리용률이 높아감에 따라 전송과정에 회사의 생명과 같은 자료들이 쉽게 보호될수 있었다.

언제나 련결된 상태에서

지난 시기 원격사용자는 본부에 있는 모뎀은행에 전화선을 리용하여 접속하여 원격으로 봉사와 접속하면 도청, 전송장애 혹은 위장과 같은데는 거의 우려하지 않았다. 호스트싸이트의 견지에서 로출을 방지하기 위해서는 보안계층이 실현되여야 하였다. 인증, 역호출, 시간제한, 접근제한들을 리용하여 통신에 대한 통제를 강화하고 위험의 가능성을 약화시켰다. 이러한 보호조치들이 가능하게 된것은 주로 통신의 1대1 성격이 있기때문이

였다. 통신이 수립되면 쉽게 찾아서 통제할수 있었다. 통신자체는 전용선으로 공공전화체계를 통과하는 동안에는 상대적으로 보호되였다.

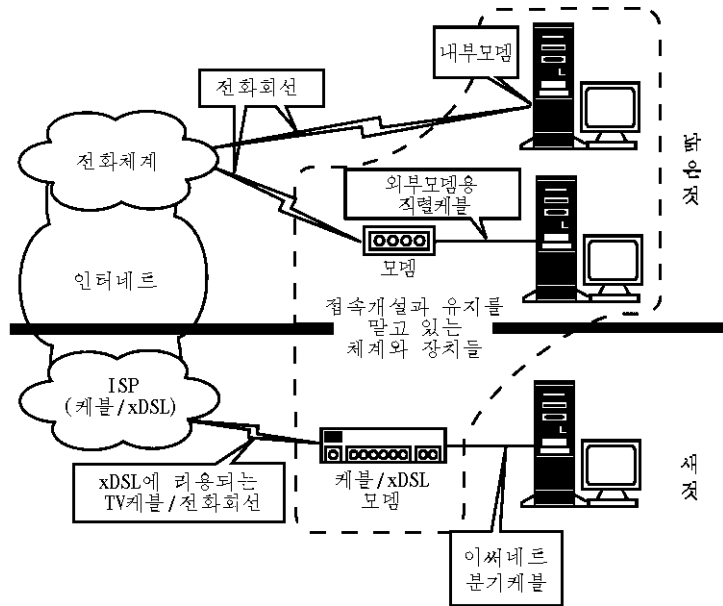



그림 12－4. 광대역에 의하여 불필요하게 된 사용자 및 체계의 접속수립

이써네트에서 접근장치에 대한 접속에 광대역기술이 리용되기때문에 콤퓨터를 켜놓기만 하면 인터네트통신을 할수 있게 된다(그림 12－4). 이것은 콤퓨터가 접속수립과 유지를 책임지고 해야 하였던 전통적인 모뎀식접근으로부터의 커다란 전환으로 된다. 현재 표준광대역으로 접근장치에 접속되면 이써네트대면부에 있는 다른 체계들의 상태에는 관계없이 인터네트로 나갈수 있다. 콤퓨터의 이써네트대면부는 사용자가 대면부를 초기화하거나 전화번호를 알거나 접속에 대하여 조심할것을 요구하지 않는다. 이 모든것은 조작체계에 의하여 조종되며 지어 IP주소는 ISP가 자동적으로 할당해 주어 사용자와의 호상관계를 더 필요없게 한다. 인터네트접속은 전적으로 그 책임이 접근장치에 달려 있어 사용자를 해방시키며 사용자의 콤퓨터를 접속유지의 부담에서 해방시켜 준다. 그 끝점체계는 단순한 망의 한마디점이다.

접근장치에 련결된 콤퓨터들은 거의 보호없이 인터네트에 련결되게 된다. 광대역제공자가 콤퓨터에 케블과 이써네트대면부를 설치하고 보안조작이 없이 콤퓨터를 련결시키는것은 매우 례사로운 일이다. 이것으로 하여 말단체계에 그 어떤 보안통제가 없이 인터네트에 직접 오랜시간에 걸쳐 련결되여 있게 된다. 차이는 크다. 인터네트상에서 이동형사용자가 잠간동안 접속했지만 ISP를 전화선상으로 찾는것, IP주소, 전송형태 지어는 그 콤퓨터위치까지 인터네트에는 오래동안 남아 있게 된다. 회사의 직접적인 원격전화선상지원과 비교해 보면 그 로출은 깜짝 놀랄만한것이다. 명백한 차이는 사용자가 인터네트에 련결되여 있는 상태에 비하여 회사가 제공하는 전화회선식련결은 점 대 점이라는것이다.

어느 한 체계가 인터네트에 련결되여 있을 때 그 형태에는 관계없이 그 체계는 무수한 위협을 받을 처지에 놓이게 된다는것은 널리 알려 진 사실이다. 또한 인터네트에 접속되여 있는 지속시간이 길면 길수록 해커들에게 발견되여 목표로 될수 있는 가능성은 더욱 커진다. 전용인터네트선로에는 대체로 방화벽이 배치되지만 인터네트에 드문드문 접속하는 호스트측에서는 그것이 잘 보이지 않는다. 그 리유의 하나는 접속의 성격 즉 움직이는 목표를 타격하는것은 훨씬 더 힘들다는데 있다. 그러나 현실은 이것이 틀리며 이중성체계들도 전용선을 가진 체계들과 꼭같이 간섭 당할수 있다는것이다. 간단히 말하여 전화회선식인터네트접속은 체계를 위험에 빠뜨리며 전용선도 꼭 같은 위험성이 있으며 오히려 시간적으로 볼 때 위험성은 더 높다는것이다. 언제나 접속되여 있든 잠간 접속되여 있든 광대역이든 모뎀이든 인터네트에 들어 가면 공격위험은 반드시 있다. 일이 바로 그렇게 일어 나는데 만약 늘 련결되여 있다면 그 사용자는 《날아 다니는 오리》가 못되고 《앉아 뭉개는 오리》로밖에 안될것이다.

회사망에로의 접근

VPN기술은 원격사용자들이 인터네트를 리용하여 회사자원에 접근하게 하는 최종적인 촉매제이다. 이것은 응당한 전진과정으로 되였다. 인터네트는 어디에나 있으니까. 전화체계와 마찬가지로 더 높은 대역너비접속들이 정상으로 되고 있으며 VPN기술은 암호화기법들과 인증으로 통신을 안전하게 해주고 있다.

VPN이 성공하게 된 요인은 지금까지 광대역기술의 도래와 리용에 있다. 그것은 고속접속이 가능하여 열람하기에 좋았으며 더 큰것들도 인터네트에서 더 빨리 얻어 낼수 있게 하였기때문이였다. 그런데 그것이 거의 전부였다. 32K 또는 56K모뎀 등을 통한 인터네트개인접속과 주로 관련되여 있던 대역너비가 거의 하루밤사이에 100배로 뛰여 올랐다. 공공전화체계와 모뎀에서 벗어 나 전용광대역선로를 가짐으로써 더 큰 접속속도를 얻게 되자 즉시 격정의 파도가 일기 시작하였다. 그러나 거의 동시에 많은 사람들이 그 봉사를 기업자원에 접근하는데 리용하려고 하였다. 접근속도가 크게 도약한데 대한 흥분이 점차 가라앉음에 따라 많은 사람들은 이것을 원격접근에 쓸수 있는 방도를 탐구하는데 눈을 돌리기 시작하였다. 바로 이 시점에서 VPN기술이 도약하였으며 기술계를 빨아들였던것이다.

원격의뢰기쏘프트웨어는 처음 나타났다. 어느 한 제품일식에는 기업의 싸이트에서 인터네트와 련결된 장치와 이동식체계에 적재된 의뢰기쏘프트웨어가 있어 인터네트로 회사의 자원에 원격접근할수 있게 되여 있었다. 원격접근대안을 해결하기 위하여 막대한 시간과 자금이 투하되였으며 지금도 계속되고 있다. 원격의뢰기접근과 보조를 맞추어 VPN에 뛰여 든것은 VPN을 종단시켜 다시한번 의뢰기체계가 통신의 부담을 벗어 버리게 하는 DSL과 케블모뎀대체안이였다. VPN은 지금 광대역접근이라는 세찬 돌개바람으로 전반적인 기술계를 휘몰아치는 불길이다.

회사망에 무제한하게 접근이 허용됨으로 하여 원격싸이트나 원격사용자들이 회사싸

이트에 설치된 정교한 방화벽과 기타 보호수단에 의하여 보호되던 자료들을 마구 복사하거나 열어 보게 되는것은 범상한 일로 되게 되였다. 많은 경우 VPN을 리용하면 원격사무원들에게 보장해 주는 비싼 자원과 방조없이 원격체계에서는 불가능한 응용프로그람들을 실행시킬수 있다. 간단히 말하면 VPN은 내부망에 있는 체계에서 흔히 할수 있는 모든것을 다 할수 있게 한다는것이다. 일부 대안들에는 Microsoft회사의 Windows Internet Naming Service(WINS)와 NetBIOS능력들을 제품에 포함시킴으로써 자원과 체계에 대한 령역열람을 마치도 회사싸이트에 앉아 하는것처럼 할수 있게 한다.

본질상 VPN은 원격활동을 내부조작으로 미끈하게 융합시키는 일종의 《만병통치약》으로 실현되고 있는 중이다. 최종제품은 통제환경의 테두리를 멀리 벗어 난 먼곳에 있는 체계에서 쓸수 있는 자료와 응용프로그람인것이다.

끝은 열려 있어

근본적으로 VPN이 제공하는 봉사는 매우 단순하다. 즉 전송중의 정보를 보호하는것뿐이다. 그렇게 함으로써 여러가지 정보통신의 혜택이 이루어 질수 있을것이다. 하나의 좋은 실례가 턴넬화(tunneling)이다. 통신의 보안을 결함없이 깨끗하게 하기 위하여 원래의 자료흐름을 교갑화한 다음에 전송한다. 교갑화공정은 보호공정과 자료전송과정을 간단하게 해준다. 우점은 여기에서 VPN에 속한 체계들이 마치도 거기에 중개자가 없는듯이 통신을 진행하는것이다. 그림 12－5에 제시된 실례는 내부망에서 흔히 작용하군 하는 데타그램을 만들어 내는 원격체계이다. 이 데타그램은 교갑화되여 인터네트상으로 회사사무실에 있는 체계로 전송되면 거기에서 원래 데타그램을 교갑해제하여(필요하면 복호화하여) 내부망으로 배포한다. 응용프로그람들과 말단체계들은 그이상 더 령리한 작업을 할수 없다.

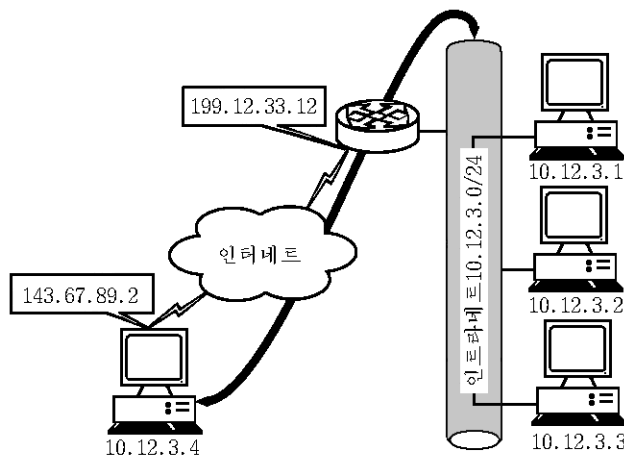



그림 12－5. 회사자료에 대한 공격자의 직접접근시도

일부 VPN실행계획들의 목표는 인트라네트봉사를 최대한 모방할수 있는 통신을 인터네트상에서 원격사용자들에게 제공하는것이다. 많은 VPN대안들이 비판을 받았는바 그것은 내부망에서나 가능한 봉사를 의뢰기체계들에 해줄수 있는 능력때문이였다. 광대역인터네트접근의 도입으로 하여 대역너비가 좁아 제한성이 있던 전화회선식대안에서 생기던 순수 사용적인 측면에서의 난관이 일정하게 해소되였다. 통신상 요구가 늘어 나는데 대응하기 위하여 많은 VPN대안들이 서로 결합되여 사용자뿐아니라 그 선로를 쓰는 응용프로그람에도 사용됨으로써 그 작용이 비교적 원활하게 되여 가고 있다. 따라서 VPN에 의하여 실현되는 보호는 실지 자료전송에만 해당되는것이다. 이것이 그 목적이기도 하다.

대부분의 경우 교갑화나 암호화전에 어떤 공정이 있는데 VPN은 다만 전송을 보호하기만 한다. 접속상태는 보호되지만 그렇다고 하여 통신이 보호되는것과는 같지 않다. 더 구체적으로 말하면 내부망들에 있는 체계들은 공동의 목적을 가지고 있는 집합체로 간주되여 방화벽이나 기타 보호수단들에 의하여 인터네트로부터 보호된다. 믿음직한 집단에서는 자료가 체계사이, 응용프로그람사이 그리고 사용자사이에서 자유롭게 오간다. VPN은 인터네트상에서의 전송에서 바로 이런 공정을 결합하여 이 공정을 보호한다. 이 과정은 련속과정으로서 잘 느끼지 못할 정도로 빨리 진행되며 전송적요구와 응용적요구를 다 만족시킨다. 결과 원격체계에 있는 알지 못할 내부사람들에 의하여 자료가 공유되고 리용된다.

접 근 점

내부봉사는 내부망에 있는 체계들이 리용할수 있게 하여야 한다고 본다. 내부망은 표준적으로 볼 때 조종, 보호, 감시되는 환경으로서 자기의 보안방책과 보안절차를 가지고 있다. 봉사와 자료에 내부적으로 접근할 때 로출 즉 그 통신에 대한 위협은 일정하게 알려 지며 일정한 수준에서 접수되기도 한다. 대부분의 기관들은 내부망에 대한 보안위협을 알고 있으며 만약 공격을 받는 경우 그 위험수준이 손해값과 정비례한것으로 예상하고 있다. 이 대부분은 사용자들에 대한 통제가 얼마 없는데 원인이 있다. 회사들은 인터네트에 비하여 내부망에 있는 사람들이 더 적고 사람들호상간의 통신이 필요하며(그래서 망이 있다.) 매 체계들은 필요하면 감시될수도 있으므로 내부자원에는 더 큰 위험이 있게 된다고 본다. 일부 통계자료들을 보면 회사자료에 대한 공격으로 내부망이 더 큰 위협을 받는것으로 나타나고 있지만 회사들에서는 자기 울타리내부통제는 잘할수 있다고 확신하는것이다. 지어는 보안방책도 없고 취약성이 있는 기관들도 아직 여유는 있으니 그에 맞게 보안방책을 실행하면 될것이라고 항상 생각만 하고 있다. 그럼에도 불구하고 인터네트는 많은 기관들에 생각했던것보다 훨씬 더 큰 위험으로 되고 있으며 일부 회사들은 그것을 현실로 체험하였다. 근본문제는 인터네트가 아직 미지의것으로서 위협은 계속될것이며 그렇기때문에 내부망에 대한 보다 예견성 있는 보안대책을 강구하여야 한다는것이다. 어느 경우에나 정보공유에도 기업의 성장자원에도 내부망이 리용된다. 바로 그러한 열린 통신을 사람들은 집에 앉아 인터네트로 하기를 바라는것이다.

VPN기술은 바라는 생각과 통제권사이의 완전한 모순의 결정체이다. 응용프로그람들, 봉사형태들 그리고 자료들이 있는 내부망은 보안관리자들이 관리하는 일정한 형태의 방화벽, 절차 및 공정에 의하여 안전하다고는 간주된다. 그러나 VPN의 본질은 기업보안과 보안태도의 인식이라는 기초적인 개념을 부정한다. 기업의 방화벽강화로 하여 격퇴 당하였던 공격자들은 원격VPN의뢰기들을 상당히 쉬운 공격대상으로 삼을수 있다.

전반적으로 보면 관리담당자들은 언제나 보안보강조치를 취하고 공정들을 갱신하며 기간체계들에 대한 전반적보안유지 및 보수를 진행하여 체계에 취약성이 나타나지 않게끔 하고 있다. 한편 이 취약점들은 말단사용자체계에 있으므로 그 사용자들은 자기 콤퓨터들을 보안관리자들만큼 높은 수준에서 관리하지 못하는것이다. 고급사용자가 전반적보호안을 도입하는 경우 많은 원격체계들은 기업전반에서 쓰는 조작체계를 가동시키지 못하여 본질적으로 불안정하게 된다. Microsoft사의 Windows 95와 98가동환경들이 현재 대다수의 개인용 즉 말단사용자급체계들에 설치되여 있으며 제한된 보안능력과 전반적인 강력성이 있는것으로 널리 알려 져 있다. 따라서 근본적인 약점이 있으면 체계에 적용된 어떤 보안도 약화될수 있다.

VPN실현이 절박한 요구로 나서지만 그 특성들의 충돌로 말미암아 회사의 싸이트에서의 보안응용기초축성은 그만 두지 않으면 안되게 된다. 사용자가 VPN을 리용하여 회사와 접속하는 순간에 벌써 인터네트의 거의 모든 측면이 보안성으로는 무효로 되고 만다. 오직 보호가 잘된 내부망이 불안정한 환경 즉 인터네트와 충돌하지 않는 경우에만 단일보호점을 적용할수 있을것이다.

보 안 봉 투

이러한 전면적인 로출 즉 공개상태에 대한 파악을 충분히 하기 위하여 방화벽과 침입검출체계라는 격납고에 의하여 인터네트와 구획 지어 진 회사망을 상상해 보자. 그리고 개인소유의 체계들이 들어 있는 건물을 무장한 경비병들이 지킨다고까지 상상해 보자. 내부망에서 자료가 공개적으로 공유되고 접속되고 있다고 가정해 보라. 그에 참가하고 있는 매 콤퓨터가 기관에 의하여 꼭같이 보호되고 통제되여 있다.

이제는 그 콤퓨터들중 하나는 통제가 없는 먼곳에 가져다 모뎀으로 점 대 점련결을 한다. 원격콤퓨터는 아직 고립되여 있고 전화체계외에 그 어떤 다른 미타한 체계에 련결되지 않은 상태이다. 통신자체는 상대적으로 닉명이며 수신방해를 논다 해도 복잡하게 되여 있다. 그러나 VPN에서 보는바와 같이 암호화를 전화체계상의 규약에 적용하면 보호가 증가된다.

다음 그 원격지에 있는 콤퓨터를 인터네트에 련결시키고 회사와 VPN을 수립한다. 그러면 회사사무실에 있던 때와는 다른 그런 위험이 로출되게 된다. 아직 그때와 같은 접근은 허용된다.

앞에서 보는 세가지 실례들에서 보는바와 같이 그 콤퓨터가 통제환경으로부터 원격지에 날라 지고 전화회선접속을 하자마자 보안상태가 급격히 떨어 지게 된다. 체계가 도

난 당하는것으로부터 시작되여 먼곳에서 전화망으로 통신되는 도중에 자료가 털리울수 있는 정도까지 그 위험은 다양하다. 그러나 그 체계와 그 정보의 전반적인 안전성은 상대적으로 보호된 상태이다. 그러나 그 원격콤퓨터가 인터네트에 가입한 때부터 위험은 기하급수적으로 늘어 난다.

첫 실례에서 체계들은 보호의 《봉투》에 있어서 보호층에 의하여 비법적인 영향을 받지 않게 고립되여 있다. 다음 그 보호봉투를 원격체계로 확장하니 불피코 봉투는 약화된다. 그러나 본질상 존재는 있으니 그 정보는 보호되여 있다. 원격전화회선접속체계로 회사의 보호환경에서 제공되였던 보호가 일정하게 소모되여 무한수의 위험에 직면한다. 그러나 중요한것은 회사싸이트를 위한 보안봉투가 그렇게 심하게 영향은 입지 않았다는것이다.

현실적으로 원격지에서 전화회선으로 내부로 망을 직접 접속하여 생기는 위험은 대체로 전화체계를 통하여 비법사용자들이 접근하고 있는것과 관련되여 있다. 회사는 원격사용자들에게 회사접근용전화번호들을 제공하는데 이 전화번호들은 지구상의 그 어느곳에서나 접근할수 있는것이다. 공격자들은 목표로 될만한 원격접근전화번호들이 있음직한 전화번호대역을 쉽게 신속히 알아 낼수 있다. 일단 그 대역을 알아 낸 다음 전화번호훑기 즉《다이얼전투》를 벌려 간섭을 얼마 하지 않고 매 전화번호들을 검사한다. 그러나 이 위험을 억제할수 있는 요소들은 현재 많다. 역호출, 고급 및 다층식인증, 확장기록, 시간제한요소들, 접근제한요소들을 잘 결합하면 공격자에게 힘든 목표로 된다. 단일접근점이 오직 하나이며 원격체계가 고립되게 되면 보안봉투는 형체를 유지하여 그대로 있게 된다. 물론 쇠퇴해 지는 정도는 회사의 단일접근점의 보안상태와 원격체계의 고립수준에 직접 달려 있다.

마지막씨나리오 즉 VPN이 배비되여 인터네트로 회사에 접속하는 씨나리오에서는 보안이(전화회선식접근방식과 같거나 혹은 보다 높지는 못해도) 상당히 높은것으로 느껴진다. 왜 그렇지 않겠는가. 특성들도 꼭 같고 보안상태도 꼭 같은것으로 보인다. 전화회선식대안들에서는 통신이 상대적으로 보호되고 회사에 있는 종단체계도 안전하고 인증대책도 제대로 있어 비법접근이 감소된다. VPN도 역시 이러한 특성들을 가지고 있으며 훈련을 잘 주면 포괄적인 보안봉투를 얻을수 있다.

그러나 VPN의 봉투는 투명봉투 즉 VPN이 하나의 규약처럼 실현되지 않으면 그만한 강도를 가지지 못하는 보안적측면이다. 회사가 제공한 봉투가 VPN에서 터질 지경으로 늘어 난다. 그 요인은 원격체계가 보안측면과 보호를 조종하게 되였기때문이다. 보안봉투가 이제는 회사에 의해 더는 제공되거나 관리되지 않고 오히려 원격체계가 이제 와서는 모든 보안을 현지에서 회사쪽에 대고 감시하고 감독하게 되였다는것은 명백해 진다.

원격체계가 인터네트와 결선하여 IP주소를 ISP로부터 받으면 인터네트세계화의 통신이 이루어 지게 된다. 인터네트상 어디엔가 회사망으로 들어 가는 VPN관문이 있어 거기에서 내부망으로 들어 가는 접근을 제공한다. 원격체계가 VPN을 구성하여 자료공유에로 들어 가면 수많은 취약성들이 나타나서 회사가 보안봉투를 제공하려고 하는 보안대책을 완전히 교묘하게 우회하게 된다. 이미 실현되였던 보안은 인터네트에 접속하는 바로 그 순간에 극적으로 뒤죽박죽이 되며 원격체계는 회사보안의 《재판관》, 《판사》 지어는 《처형자》가 된다.

원격체계는 매우 강력한 VPN해결책 즉 호스트체계가 경로기로서의 역할을 놀지 않고 인터네트에서 개별망으로 정보를 전송시키는 VPN방안을 채용하였을수도 있다. 좀 더

설명하면 그 VPN방안은 내부망으로 들어 가는 접근을 제한하기 위하여 제한된 방화벽기능이나 려과기능을 리용할수 있다는것이다. 그러나 이 VPN의뢰기나 방화벽쏘프트웨어에 의한 보호는 사용자가 해제해 치울수 있으므로 결국에는 공격 받을수 있게 되여 있다. 사용자가 보호를 해제할수 없는 종합대안을 실행하는 경우에는 짐작컨대 취약점이 하나 생기면 그것을 보강퇴치할수 있을것이다.

제한된 수의 방화벽을 가지고 보안관리자들이 지탱해 보려고 애 쓰는 울타리와 방화벽에 있어서 이런 씨나리오는 매우 례사로운 일이며 거의 매일 일어 나는 일이다. 방화벽에 대한 기관들의 관심이 없어 진 조건에서 원격체계의 방화벽쏘프트웨어에서 취약점들이 발견되면 보안의 와해가 어떠해 지리라는것은 짐작하기 어렵지 않다.

취약성의 개념

충분한 기술과 공정에 의하여 마련되였던 회사의 보안이 파괴되는 극단적인 경우를 잘 리해하기 위하여서는 원격체계가 인터네트에 공개되고 로출된 체계라는것을 알 필요가 있다. 일부 경우 광대역에서도 마찬가지로 로출상태는 항시적이며 오랜시간동안이여서 공격자에게 가장 큰 기회를 줄수 있게 된다.

인터네트는 불피코 위험의 바다이다. 그것은 인터네트에 방대한 인적, 기술적자원이 있어 해커들이 닉명으로 남에게 특히 준비가 없는 사람들에게 큰 재난을 들씌울수 있기때문이다. 통신의 여러 층에서 사용되고 영향을 미치는 공격방법에는 여러가지가 있다. 실례로 봉사거부(DoS)공격들은 그 어떤 체계나 봉사를 완전히 마비시키는것으로서 그 목적은 순수 파괴이다. DoS공격들은 규약의 취약점과 같은 낮은 준위통신속성에서의 약점들이나 응용프로그람자체에 있는 높은 준위약점들을 교묘하게 리용한다. 일부 다른 공격들은 응용이 매우 독특하여 정보에 대한 접근이나 정보입수를 위한 특수한 환경에 쓰는것도 있다. 이러한 공격들이 응용오유나 이상동작들을 교묘하게 리용하는것은 점점 범상한 일로 되고 있다. 결과 체계정보를 획득하거나 지어 호스트체계를 원격조종하기 위한 전용응용프로그람들이 나오고 있는것이다.

트로이목마들은 매우 교묘해 지고 쓰기 편리하게 되였다. 그것은 주로 흔히 쓰는 조작체계들에 커다란 약점들이 있으며 매우 유능한 프로그람전문가들이 많이 나오는것과 관련되여 있다. 인터네트에 련결되여 있는 어느 한 콤퓨터에 트로이목마가 설치되여 있으면 그것을 리용하여 그 콤퓨터에 침투하여 원격조종도 하며 자료도 손에 넣을수 있고 건반입력도 모두 알수 있을뿐아니라 언제 그 콤퓨터가 인터네트와 접속하기 시작하여 언제 접근할수 있는가를 공격자가 쉽게 알수 있게 된다. 일부 경우에는 인터네트에서 떨어진 상태에서도 정보를 다 수집하였다가 그 콤퓨터의 인터네트접속이 수립되면 제꺽 공격자에게 그 수집내용을 보내오게도 할수 있다. 바로 이 취약성을 최악의 씨나리오라고 볼수 있으며 실지 가정용콤퓨터가 피해 보는것은 례상사로 되여 있다.

트로이목마가 설치되지 못하거나 혹은 완전히 실행되지 못하는 경우 림시적으로라도 공격자는 접근권을 얻어 목표로 된 그 콤퓨터나 그 사용자에 대한 사활적인 정보를 수집할수 있으며 결국 계속 그런식으로 공격하여 더 큰 결과를 얻을수 있다. 항비루스프로그

람들과 호스트용방화벽프로그람들이 취약성을 줄일수 있으며 취약성을 발견할수도 있으므로 잘하는 경우 그것들을 제거할수도 있다는것은 론의해 볼 여지가 있다. 이러한 프로그람들의 실행, 유지보수, 안전한 일상적인 가동은 전적으로 사용자들의 손에 달려 있다. 그러나 전문일군들이 있는 고도로 기술적이며 정교한 체계들의 환경을 보호한다는것은 상당히 복잡한 일이며 인터네트전체에 널려 있는 원격체계들은 더 말할 필요도 없다.

일 보 후 퇴

인터네트도입초기에 콤퓨터들은 공격을 받아 비법접근되고 자료가 도난 당하거나 사적소유의 정보들이 공개되군 하였다. 위협이 더 커졌으며 보다 지능화되고 근절하기 곤난하였으므로 공격에 직접 걸려 들지 않기 위하여 방화벽을 설치하였다. 또한 그와 병행하여 일부 봉사체계들은 전반적보호를 가일층 높이도록 약점에 대처하여 강화되였다. 또한 이 강화된 전용체계들을 DMZ라고 하는 고립된 망에 배치하여 그 체계에서 개시되는 공격으로부터 내부망을 보호하게 하였다. 이 모든 대책들을 취하였지만 해커들은 오늘까지도 내부체계에 대한 공격을 놀랄만큼 계속 하고 있는것이다.

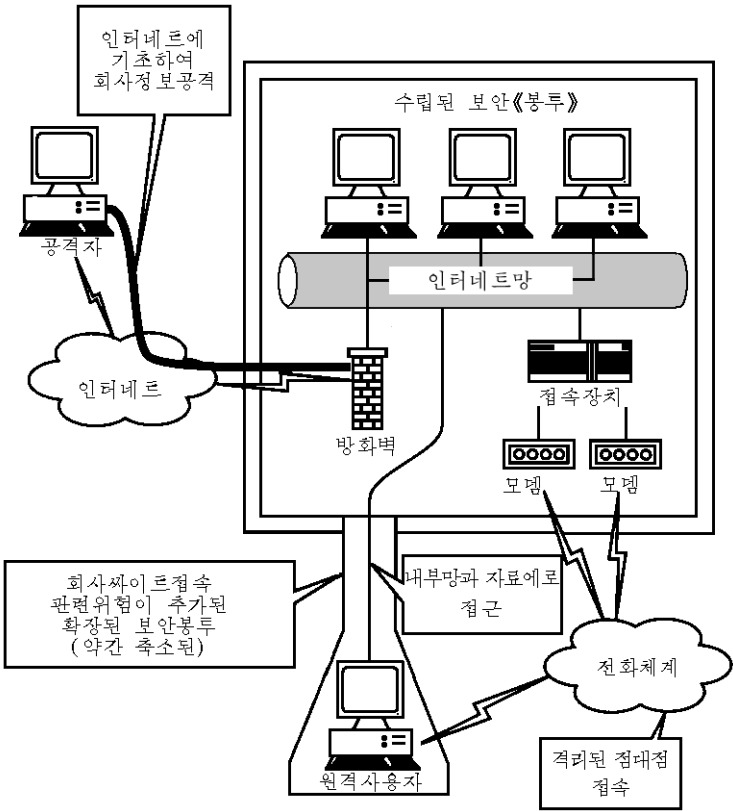



그림 12—6. 회사자료에 대한 공격자의 직접접근시도

오늘 방화벽은 인터네트망접속에서 근본적인 내부비품으로 되고 있으며 일부 기관들에서는 대량적으로 설치하여 방대한 수의 콤퓨터들과 망들을 보호하고 있다. 이것은 하나의 관례로, 인터네트생활의 기정사실로 그러나 비용이 많이 드는것으로 되고 있다. 내부체계와 자원들을 인터네트로부터 보호하는것은 가장 중요한 일이며 여기에 방대한 로력과 자금이 투입되군 한다.

론리적으로 보면 이렇게 실현된 대부분의 보호조치들은 사적소유의 자료나 정보가 공개되거나 변경되거나 파괴되지 않게 보호하는데 목적이 있다. 여기서 그 자료는 보안대책에 의하여 만들어 진 보안봉투속에 남아 있다. 따라서 그 정보를 얻기 위하여 공격자는 운영조건들을 침투, 우회 혹은 조작해야 한다(그림 12−6을 보라).

VPN의 출현으로 원격체계는 알려 진 위험들과 위협의 테두리내에서 회사자료에 안전하게 접근하게 된다. VPN이 통신을 보호하며 보안을 회사로부터 밖으로 나가 원격지까지 확장할수 있다고 생각할수 있다. 그러나 이 생각은 VPN의 기본구성인 인터네트를 홀시한데서 나오는것이다. 그림 12−7에서 보는바와 같이 공격자는 일반사용자에게 완전히 장악된 체계에 있는 회사자료에 접근한다. 그 체계는 축적된 경험과 기술의 보호를 받지 못하고 있다.

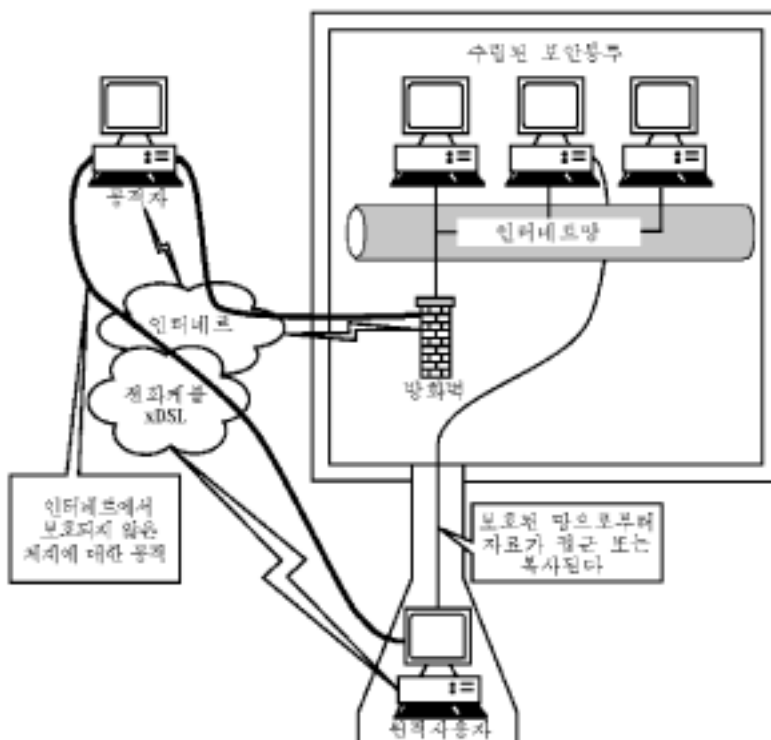



그림 12−7. 공격자는 인터네트의 덜 보호된
접근점으로부터 자료를 얻는다.

공격자의 견지에서 그 정보는 회사가 인터네트에 접속상태이므로 인터네트상에 있는것이다. 따라서 접근공정과 접근매체는 변함이 없고 다만 보안수준만 다를뿐이다. 결국 그 정보는 공격자에게 주어 졌으며 보다 상당히 복잡한 통로를 거쳐야 하는 직접적인 접근은 필요 없다. 인터네트접속만 아니라면 원격호스트들의 기능, 속도, 보호는 모뎀에 기초한 기성원격접근에 비하여 상당히 높은 수준이였을것이다. 아쉽게도 인터네트는 기능을 확장시켜 주는 좋은것이지만 결국에 가서는 불안전한 망이기도 하다.

론리적으로 볼 때 이것은 정보보안의 비극이다. 인터네트의 보안과 그 위험성해소를 위하여 얼마나 막대한 시간과 자금을 들이고 연구를 하였는지 모른다. 기초적인 경로기려과, 방화벽, 침입탐지체계로부터 시작하여 체계경화, DMZ, 공극(air–gap)들에 이르기까지 수많은 기술의 벽돌로 보안이라는 커다란 벽도 쌓아 놓았다. 인터네트를 겨냥한 방위체계가 파잉되였으므로 이것으로 하여 공격자들은 다른 통로를 취하게 되여 원래 빠져들던 함정이나 덫을 피하여 우리의 가장 약한 허점으로 쳐들어 오고 있다.

공격이 상당한 요새에 부딪쳤을 때 그 방향과 형식을 바꾸는것을 보면 중세기의 전쟁을 방불케 한다. 침입자들을 격퇴하기 위하여 높은 성벽을 쌓아 성새를 건설하였다. 주변수로에 물도 채우고 함정들도 파놓고 치명적인 곳곳에는 교묘한 장치를 해놓아 적들의 공격을 저지시키게 되여 있었다. 이 성벽의 일부 장소들 특히 수로밑에는 비밀관문을 설치하여 정찰병들이나 간첩들이 성새를 빠져 나가 정보를 가져 오든가 아니면 봉쇄때 물자들을 날라 들이군 하였다. 현실은 바로 이것을 반복하는것이다. 지금과 옛날전쟁사이에 차이나는것이 있다면 옛날에는 적에게 중요한 정보를 가지고 있는 장수나 보좌관 혹은 그 어떤 사람도 성밖으로 나가지 못하게 하였다는것이다.

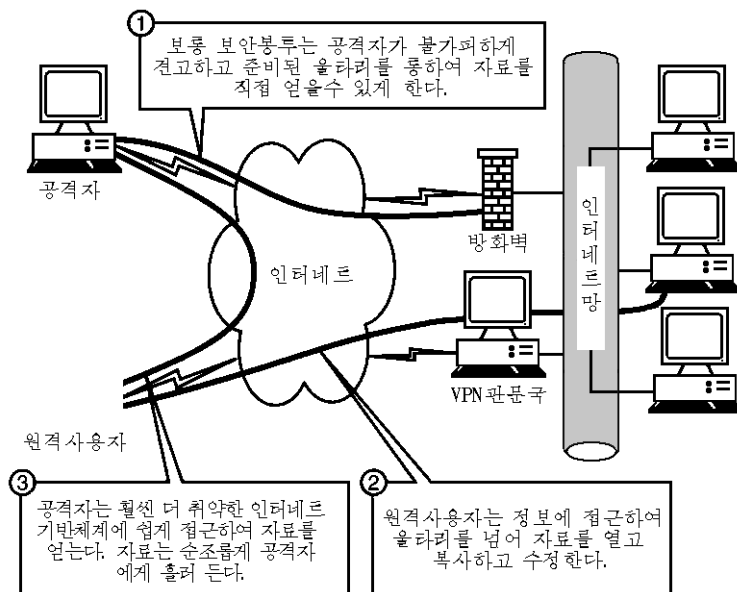



그림 12－8. 자료접근은 취약성이 있고 인터네트관련위험요소들이 있는 체계에서 가능하다.

완전히 대조되게 지금은 회사 각층의 사람들이 밖에서도 정보에 접근한다. 이것은 관문을 거쳐 성밖으로 공격계획을 가진 장수를 내보내서 아무런 호위도 없이 자기 천막에서 홀로 그 공격계획을 연구하는것과 마찬가지다. 적측에서 그 장수를 덮쳐 직접 성새에 들어 가지도 않고 그 정보를 얻는것은 식은죽먹기일것이다. 사실 오늘날의 공격자는 희생자를 제 마음대로 교묘하게 조종하여 자료를 쉽게 고치고 수집할뿐아니라 그 소유자는 무슨 일이 진행되였는지 모르게 할수도 있을것이다. 그림 12－8에는 거의 저항없이 들어 갈수 있는 통로가 어떻게 만들어 지는가를 보여 준다.

미궁같이 복잡한 방위체계들이 건설되여 적을 정면으로 겨누고 있지만 정보는 밖으로 계속 새나가고 있다. 결국 잘 만들어 놓은 보호벽이 거의 무용지물로 되고 있는셈이다. 이전에 몇개의 방화벽이 단일입구점을 가지고 내부망의 정보를 보호하였다면 지금 보면 방화벽이 없이 수천개의 입구점이 나 있을것이다. 우리는 일보후퇴하였을뿐아니라 방화벽에 의한 문제점들도 그 규모가 상당히 커졌다. 인터네트를 도입한 초기에는 방화벽이 없이 단일한 인터네트접속이면 충분하였다. 오늘 기관들은 여러개의 인터네트접속에다가 복잡한 보호조치까지 취해야 한다. 원격콤퓨터와 자그마한 가정사무실들을 위해 VPN을 형성함으로 하여 통제하기 어려운 수천개의 인터네트접속점들을 가지고 있는셈이다.

해커침습실례의 한가지

어느 금요일 저녁쯤 큰 국가건설회사의 기사장으로 일하는 한 친구로부터 나에게 전화가 왔다. 그는 자기의 콤퓨터가 말을 잘 듣지 않든가 주말에 낚시질을 하자든가 할 때면 의레히 전화를 걸어 오군 하였다. 그러나 이 전화는 시작부터 완전히 달랐다. 그는 자기가 해커의 침습을 당한것 같다는것이였다. 하드구동기가 밤새 늦게까지 돌더니 최근에 새로 설치한 블랙아이스(BlackIce)가 상당한 량의 영문 모를 전송량을 기록하더라는것이다. 그가 모뎀케블과 VPN을 리용하여 밤 아니면 낮에 집에서 일을 보는데 그것은 과잉전송량과 일반사무실들의 방해를 피하기 위해서라는것이였다. 또한 Windows 98을 조작체계로 표준프로그람들을 써서 자기 일을 한다는것도 이야기하였다. 또한 그는 늘쌍 콤퓨터를 켜놓는다는것이였다. 그렇게 못할것도 없지.

해커의 공격을 받았다는것을 완전히 확신한 나는 그에게 그 콤퓨터를 다치지 말고 놔두고 그의 집망에 있는 다른 콤퓨터를 리용하여 엿보기도구(sniffer)를 가동시켜 신호상에서 무슨 일이 진행되는가를 보라고 하였다. 몇분후에 그의 콤퓨터와 어느 한 인터네트상의 호스트사이의 통신이 시작되였다. 전송내용을 똑똑히 본후에 그의 콤퓨터에 외부접속이 진행되고 있다는것이 명백해 졌다. 그의 경험으로 봐서 또 그가 그 콤퓨터에 설치한 여러 쏘프트웨어로부터 만들어 지는 기록파일들 그리고 그와 같은 처지에 빠졌던 다른 친구들의 이전 경험으로 봐서 나는 그의 콤퓨터가 접근을 당하고 있다고 생각했다. 나는 케블모뎀에서 그 이써네트를 다 뽑게 하였다. 그리고는 문제의 심각성이 어느 정도인가 즉 그 콤퓨터에서 대체 가지고 싶어 하는것이 무엇인가를 물어 보았다.

몇마디의 말을 통해 보니 해커가 회사마크, 이름, 계약정보, 경쟁력분석, 계획시간표,

가격비교까지 다 붙어 있는 전국적인 건설계획 입찰자료전반을 다 접근하고 있었던것 같았다. 이런 정보를 수집하여 조사해 봄으로써 품질검사와 공학적문제를 해결하는것이 바로 그의 일이였다. 더 말을 주고받아 보니 사업습관과 보통기억력으로 그 자료를 언제 마지막으로 접근하였는지 알고 있는것 같았다. 바로 그래서 그는 기계가 한참 일을 하고 있어 나에게 당장 전화를 걸려고 했다고 하는것이였다. 나에게 큰 일도 아닌것을 가지고 놀라게 할가봐 항비루스프로그람과 무료쏘프트웨어를 먼저 돌려 볼가 하였다는것이였다. 결국 우리는 콤퓨터에 들어 가 무엇이 언제 접근되였는가를 확인해 볼것을 결심하였다.

우리가 처음으로 발견한것은 plug–in이 있는 BackOrifice였는데 그것을 보니 그 친구를 특별히 겨냥한 공격 같지 않았고 누군가가 인터네트상에 앉아서 활짝 열려 진 Windows체계에 대하여 장난질을 하려고 한것 같았다. 우리는 매 파일의 접근시간을 조사하기 시작하였다. 몇주일전 날 밤중에 접근한것들이 많았다. 더 조사해 보니 그가 얼마 전에 받았던 의심되는 전자우편들과 숨은 디렉터리들이 나타났다. 그러자 나는 중지시키고 그에게 최악의 경우를 고려하여 체계의 다른 그 무엇을 노린것이 없겠는가고 그에게 물었다. 통과암호도 없는 그의 TurboTax자료기지의 예비본이 있고 그외에 최근에 로임인상 받은 자기 부서내의 성원들의 인사문건들이 있다는것이였다.

전화로 우리는 약 세시간 이야기했는데 그것이 전부이다. 그가 자기 사장에게는 참으로 고통스럽게 전화했을것이며 아마 나와 한 전화보다 더 오랜것같이 느껴졌을것이라고 생각한다. 이것이 그의 잘못인가. 회사가 그에게 인터네트접속과 VPN쏘프트웨어를 주었고 집에서 인터네트접근하는것을 장려하였다. 그와 그의 사장에게는 이것이 론리적인것이였다. 그는 연구에 필요해서 인터네트에 접속하였고 사실 사무실에서보다 집에서 일을 더 많이 제꼈다. 그러나 정보를 채기 위하여 고용된자 아니면 우연히 노다지를 만난 스크립트장난군일수도 있는 그 공격자는 극비에 속하는 그 자료에 접근하였다. 이러나저러나간에 어쨌든 사고가 났으니 몇년간은 사업에 영향을 미칠것이다.

해 결 책

VPN의 실행으로 인하여 생기는 보안상 문제점들은 쉽게 해결될수 있다. 고도로 발전된 기술을 가지고서는 해커들의 공격을 막아 낼수 있다. 해커들은 아무리 중무장으로 보호된 망에도 비교적 쉽게 계속 접근한다. 이러한 접근이 가능한것은 설계상 오유, 유지보수에서의 빈틈, 설정상 결함 혹은 단순한 무지에 기인된다. 어쨌든 울타리에 대한 집중경비에도 불구하고 비법접근은 놀라운 속도로 계속 일어 나고 있다. 인터네트상에 원격콤퓨터가 수백대가 있다고 가정해 보면 어떻게 해야 이 콤퓨터들을 보호할수 있겠는가. 최상의 노력을 기울였음에도 불구하고 내부망을 보호할수 없다면 가정용콤퓨터들과 이동형콤퓨터를 보호할 희망은 희박한것이다.

보안실천에서 흔히 그러하듯이 정보보안에서는 보안방책이 사활적인 역할을 한다. 자료접근에 대한 제한조치들과 정보교환을 위한 운영파라메터들을 설정해 놓으면 정보의 로출을 크게 줄일수 있다. 다른 말로 말하면 일종의 정보가 원격사무에 필요 없다고 간

주되면 원격접근체계는 그 정보나 그 체계에 접근하지 못하게 되여야 한다. 원격접근체계가 좁은 접근권을 가지면 자료는 원천적으로 보호될수 있다. 원격사용자들이 실지 접근할수 있는것이 무엇인가를 한정해 주는 역할은 VPN에서 내부망을 보호해 주는 VPN장치 바로 뒤에 있는 방화벽에서 해준다. 그러나 이 설계는 큰 제한성을 가지고 있으며 접근유연성측면에서 VPN규모조절에 제한을 주고 있다. 다른 하나의 가능성은 VPN접근장치에 쓰이는 려과방법이 있을수 있다. 려과기를 보면 내부망에 쏴 넣은 전송자료들을 통제할수 있고 일부 경우에는 려과장치를 리용하여 실지사용자인증이나 실지 그룹인증도 가능케 할수 있을것이다.

접근을 아무리 제한시킨다 해도 원격사용자가 기밀정보를 필요로 할 경우도 있을것이며 사용자에게만 봉사를 하는 사람들도 누구든지 그러한 《특수한 경우》를 목격하였을것이다. 따라서 여기서는 기술을 개입시켜 정보를 보호해야 한다. 내부망을 인터네트로부터 보호하기 위하여 방화벽에 매달렸을 때 원격체계가 내부정보를 파일들에게 넘기지 못하게 하려면 다시 기술에 의거할수밖에 없다. 호스트용보호쏘프트웨어들을 리용하는것은 완전히 새로운것은 아니다. 그러나 개인콤퓨터에 대한 공격이 계속 증가하게 됨으로써 이러한것이 있다는것이 널리 알려 지게 되였다. 그러나 이것들은 전반적인 유연성 있는 중앙조종체계식 혹은 보안관리용해결책은 못되며 다만 해당 콤퓨터에만 해결책으로 된다. 결국 매 사용자가 자기체계의 보안을 책임져야 하는것이다.

결 론

VPN의 가치는 거대하다. VPN은 시간과 자금을 절약하고 접근의 범위를 확대하며 통신에서 최대의 유연성을 보장해 준다. 그러나 VPN이 제공하는 개별적인 련결고리는 공격자들에게 가상뒤문을 열어 줄수 있다. 기밀자료들이 VPN을 거쳐 나가게 허용하는 기관들은 보호내부망에서는 보지 못하던 수많은 위험들이 그 정보들을 내맡기는것이나 같게 된다.

VPN제품들은 현재 그 종류가 많으며 접속수립방식, 접속유지방식, 내부망에서 흔히 보는 봉사들을 제공하는 방식에서 다 특성들이 있다. 만일 원격체계가 VPN을 통한 중앙사무실과의 전용통신용이 아니라면 그 체계는 상당한 취약성을 가지고 있는것으로 볼수 있다.

인터네트는 우리의 생활과 일상생활의 곳곳에 깊숙이 침투해 들어 왔다. 그러나 실지 생활과는 일정한 계선이 항상 있었다고 말할수 있다. 방화벽, 모뎀, 경로기, 려과기 지어 열람기와 같은 쏘프트웨어들은 인터네트에로 들어 가는 보이는 접근점일수 있다. 기술이 보다 발전하게 됨으로써 인터네트와 개별망들사이의 계선은 점점 흐려 질것이다. 그러나 앞날을 정확히 내다 보지 못한다면 보안방책과 위기완화과정들은 정보테로주의에서의 발전에 따라 서지 못할것이다. 계획과 통제를 잘하지 못하면 안전해 보이는 요새통로 하나만 보고 다른 보호대책은 다 홀시할것이다. 그렇게 되면 요새의 성벽들은 직접적이 아닌 공격에는 무력하게 될것이다.

제１３장. 전자우편보안

클래이 랜덜

첫 전자우편이 진행된것은 그 어떤 콤퓨터망이 제대로 리용되기전이였으므로 하나의 여러 사용자콤퓨터체계의 각이한 사용자들사이의 통신에 국한되여 있었다. 전자우편이 고안된것은 통신을 표준적이며 조직적이며 기능적인 과정으로 하기 위해서이며 보안상 문제점들을 극복하기 위해서였다.

전자우편이 사용되기전에 사용자들은 자기체계의 일정한 공간내에 공통접근구역을 떼놓아 다른 사용자들이 거기에 통보문이나 파일들을 《떨구어 놓게》 하였다. 필요한 기술적상식이 없는 사용자들이 있음으로 하여 비사용적조건들(불충분한 특권들)과 보안상 문제점들(과잉특권들)이 생기게 되였다.

대중적요구와 가능성이 있음으로 하여 일정한 기초적인 형태의 전자우편응용프로그람은 거의 모든 콤퓨터조작체계의 표준부품으로 인차 제공되게 되였다. 콤퓨터응용프로그람들은 인차 체계호상간의 전자우편교환능력을 가지게 되였다.

처음으로 상업화되고 널리 전개된 대중적콤퓨터망은 ITU X.25파케트교환망표준에 기초하고 있었다. 보다 많은 회사들이 싸이트들사이에 련결됨으로써 비록 처음에는 통신이 거의나 국부망에 국한되여 있었지만 이것은 전자우편에 재빨리 적용되여 이 망들에서 콤퓨터체계들사이에 통보문전송능력을 부과하였다. 처음에는 서로 다른 판매업체의 체계들사이 통보문전송을 할수 있게 표준화가 되지 못하였고 여러 기관망환경에 알맞는 관리 및 보안조종이 부족하였다.

처음 이 망들에서 사용된 전자우편체계의 국제표준화도 역시 ITU에 의하여 제안되였는데 X.400(1984, *Red Book*)이였다. 이것은 큰 상업 및 정부기관들속에 널리 채용되였다(비록 보다 작고 원시적인 인터네트의 형태가 존재하였고 그에 의하여 오늘도 여전히 인터네트전자우편의 기초로 되는 전자우편표준이 이미 개발되였음에도 불구하고 그 당시의 대중적《인터네트》NFSnet의 상업적리용은 명백히 금지되였다.).

X.400표준의 작성자들은 조종, 보안, 운영기관을 다계층화해야 할 필요성을 인정하였으며 나라별, 행정관리령역(ADMD: Administrative Management Domain)별, 사영관리령역(PRMD: Private Management Domain)별, 기관별, 산하단위별로 빈틈없이 계층화된 설계를 해놓았다. 그들은 또한 여러 쏘프트웨어판매업체들간 운용호환성, 통보문형식화에 대한 규약, 봉사기간통신, 의뢰기들과 봉사기간통신 그리고 비본문요소(팍스화상, 음성, 비데오 등) 첨부능력과 같은 추가적인 성능들을 확정하기 위한 끊임 없는 세부표준들의 필요성을 인식하였다.

초판의 약점과 결함을 검토처리하고 방대한 량의 조작성능묶음과 서로 구별되면서도 련관된 디렉터리표준을 첨부한 X.400표준의 재판이 나왔는데 그것이 바로 X.500(LDAP가 기본적으로 부분집합)이였다.

보다 새로운 ITU표준이 널리 전개되기전에 인터네트는 이른바 상업화에로 나갔으며 콤퓨터망으로서 이미 있던 X.25망들을 재빨리 따라 잡았다. 몇해동안 이 두 체계는 관문

체계를 매개로 함께 리용되였다. 이상하게도 상대적으로 원시적이고 단순한 인터네트전자우편표준들은 고급하고 복잡한 X.400표준이 보다 정교할뿐아니라 통신에 TCP/IP를 리용할수 있었지만 그것을 밀어 내였다.

현재의 인터네트전자우편표준들은 4개의 기본령역을 포함한다.

- **SMTP(Simple Mail Transfer Protocol)** RFC–821에서 처음으로 규정되고 다른 RFC들에서 확장된 이 규약은 전자우편봉사기들사이의 통보문전송방식을 규정한다. 초기에는 전송흐름경로조정(traffic routing)측면도 일부 규정하였지만 아래에 서술하는 DNS의 기능들이 그것을 대신하였다. 의뢰기워크스테이션으로부터 통보문을 제출하는 사용자인증방법을 제공하는 ASMTP(Authenticated SMTP)확장 즉 RFC–2554는 보안에서 특별히 중요하다.
- **《ARPA인터네트본문통보문형식표준》** RFC–822에 처음으로 규정되고 다른 RFC들에서 확장 및 수정된 이 표준은 교환될 통보문의 형식을 정의한다. 특별히 중요한것은 비본문정보를 포함하는 다구성통보문부호화표준방법을 규정하는 MIME(Multipurpose Internet Mail Extensions)이다.
- **DNS(Domain Name System)** DNS의 초기목적은 인터네트 IP주소를 콤퓨터이름과 관련시키는데 있었다. 이 체계는 SMTP전자우편경로조정에로 확장되였다. 현재 인터네트상에서 전자우편경로조정의 두번째 확장판인 MX(Mail Exchanger)레코드가 사용중에 있다. 이 확장판들은 SMTP에서 처음으로 정의된 경로조정을 대신한다.
- **S/MIME(Secure/MIME),PEM(Privacy Enhancement for Internet Electronic Mail).** 이 표준안들은 전자우편내용의 암호화 및 복호화, 통보문통합보호, 원본의 부인방지 등을 포함한 여러가지 암호화특징들을 참작한다.
- 또한 다음 2개의 표준안들은 전자우편의뢰기가 봉사기로부터 우편을 복귀하도록 하기 위하여 만든것이다.
- **IMAP(Interactive Mail Access Protocol)** 이 규약은 전자우편의뢰기와 봉사기들사이에서 의뢰기/봉사기호상작용을 위한 표준들을 정의한다. 이것은 현재 열린표준전자우편체계에 대한 사실상의 표준이지만 많은 전용전자우편봉사기체계들에 대한 교차적인 접근방식으로도 쓸모 있다. IMAP은 의뢰기의 전자우편통보문보관고상에서 수정, 삭제, 봉사기기반검색, 폴더들사이에서 통보문들의 재정리, 통보문상태조종, 공동폴더공유 등과 같은 광범한 조종을 할수 있게 한다.
- **POP(post office protocol)** 이 규약은 전자우편의뢰기가 봉사기로부터 머리부 또는 통보문을 검색하는 방법, 봉사기로부터 통보문의 삭제요청방법 들에 대한 표준을 정의한다. 이것은 아직도 널리 리용되고 있기는 하지만 아주 작은 의뢰기와 봉사기의 실현에 국한되여 있으며 큰 체계들에서는 IMAP에게 밀려나고 있다.

중요한것은 이 규약중 어느것도 배포해야 할 새로운 통보문제출방법을 제공하지 않

는다는것이다. 이 표준안들에 기초한 전자우편의뢰기는 새로운 통보문을 의뢰하는데 SMTP를 리용한다.

목 적

보안방책과 계획, 기술, 장치들이 그 기능을 심히 제한하지 않도록 하거나 보다 쉽게 응용하는데 방해되지 않도록 기본설계목적의 중요성을 고찰할 필요가 있다.

명백히 전자우편의 목적은 사용자들사이의 통신을 보장하자는데 있는것만큼 그 응용에 있어서 사용의 편리성과 신뢰성이 중요한것이다. 전자우편응용프로그람은 그 시초부터 다음과 같은 세개의 기본요소들을 포함하고 있었는데 그것들은 현재의 모든 전자우편응용프로그람에서도 여전히 찾아 볼수 있다.

- **표준형식** 표준통보문형식은 임의의 사용자가 임의의 다른 사용자와 통보문을 교환할수 있게 한다.
- **구성** 모든 통보문들은 발신자(from), 수신자(to, 경우에 따라 cc 혹은 bcc), 제출날자, 기본내용과 같은 마당들을 포함한다.
- **보안** 사용자들은 자기 우편만 읽을수 있으며 자기들이 만드는 통보문은 자기 구좌로부터의 발신으로 확인된다.

현재의 전자우편체계에는 세가지 기본요소들이 여러가지 방법으로 리용되며 다음과 같은 두가지 새로운 기초요소들만이 더 첨부되였다.

- **운용호환성** 개별적콤퓨터체계망들사이의 통보문교환능력
- **비본문정보전송** 음성, 비데오, 정화상, 자료기지, 표처리(spreadsheet), 실행파일, 스크립트 등과 같은 콤퓨터자료형을 포함하거나 첨부하는 능력

그러나 이 두가지 목적들은 자주 보안과 직접 충돌을 일으킨다.

보안목적목록으로부터 보면 다음과 같은 대부분의 콤퓨터보안령역과 관련된 일반요소들이 있다.

- 합법적사용자들만이 체계와 봉사에 접근할수 있도록 콤퓨터자원에로 접근조종을 하는것
- 자료의 류실 또는 파손의 방지
- 자료 또는 봉사의 도난방지
- 부적합한 자료보급의 방지
- 규칙 또는 기관의 방책에 따라 동작하는가에 대한 감시

전자우편통신에서의 위험과 문제점

일반적으로 전자우편체계는 인터네트상에서 한 기관의 사용자들이 다른 기관의 사용자들과 통신할수 있게 할것을 요구한다. 이것은 결국 인터네트와 그 기관의 전자우편봉사기들사이의 통신을 요구하지만 전자우편봉사기들과 인터네트사이의 직접적인 망접속은 요구하지 않는다. 인터네트로부터 특정한 기관의 전자우편봉사기들에로의 망접속을 제한하기 위한 한가지 방안은 인터네트(또는 다른 불안전한 망)와 그 기관의 내부망사이에 표준《요새》망을 배치하는것이며 우편중계장치는 요새망우에 설치되여야 한다는것이다(그림 13－1참고).

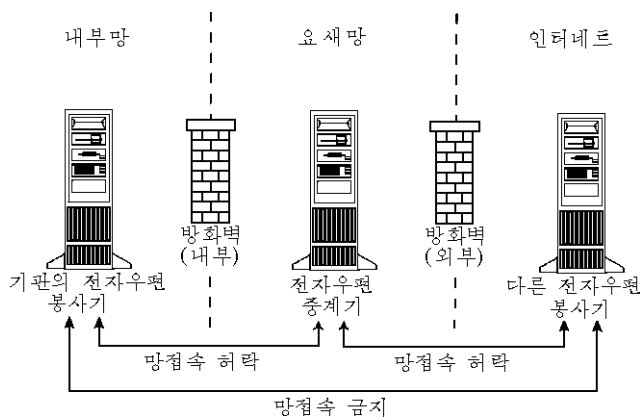



그림 13－1. 인터네트로부터 전자우편봉사기들에로의 망접속제한

외부방화벽은 전자우편중계체계에 대한 일부 보호를 진행하는 한편 전자우편중계기와 외부봉사기들사이의 일부 통신을 허용한다. 해커들은 제공되는 전자우편통로를 통하여 공격을 시도할수 있는 기회를 얻는다.

요새망에 중계체계가 실현됨으로써 제공되는 보호는 다음과 같다.

- 전자우편중계체계는 인터네트로부터 직접 공격 받을수 있는 유일한 체계이므로 내부망우에 여러개의 전자우편봉사기가 있다고 하여도 침입검출부하는 그 체계에만 집중된다.
- 중계체계를 뚫고 들어 온다 해도 거기에는 일시적인 통보문들만이 들어 있다.
- 중계기에 대하여 가해 지는 봉사거부공격은 정상동작하는 기관내부의 전송흐름을 막지 못한다.

일반적으로 공격자들은 단지 제한된 손상이나 주고 내부사용자와 외부사용자들사이의 봉사를 교란할수 있다. 해커는 중계봉사기를 완전히 손상시킬수 있는 능력을 가지려고 하며 또 내부우편중계기들을 직접 공격할수 있는 환경으로서 그것을 리용할수 있는

능력을 키우기 위하여 시간과 노력을 아끼지 않을것이다.

일부 방화벽판매업체들은 단일방화벽안에서와 류사한 기능을 제공한다. 이 기능이 실행되면 방화벽은 그자체가 전자우편중계기의 역할을 한다. 확고하지는 못하지만 기능적인 해결책은 요새망의 내부에 존재하는 중계기체계를 분리하는것인데 그것은 불안전한 망과 내부우편봉사기들사이의 직접적인 망통신보장에 아주 좋은 방법이다.

많은 경우에 인터네트상에 돌아 다니는 전자우편통보문들은 제3자의 감시로부터 보호되여야 할 극히 신중한 정보를 포함한다. 인터네트에 접속할 때 유일하게 준비되여 있는 해결책은 암호화이다. 그러나 전자우편암호화에 대한 여러 표준안들이 경쟁적으로 존재하고 있지만 어느 표준안도 현재 광범히 채용되지 못하고 있다. 정보의 전체 량과 사용자의 분포에 의존하여 암호화를 진행하는 여러가지 방법이 있다.

최대의 보안은 매 사용자의 전자우편의뢰기쏘프트웨어에서 제공하는 암호화기능을 리용하는것이다. 그림 13－2에서 보는바와 같이 매 통보문들은 송신자의 체계안에서 암호화되며 수신자체계의 의뢰기쏘프트웨어에 도달할 때까지 암호화된채로 남아 있게 된다.

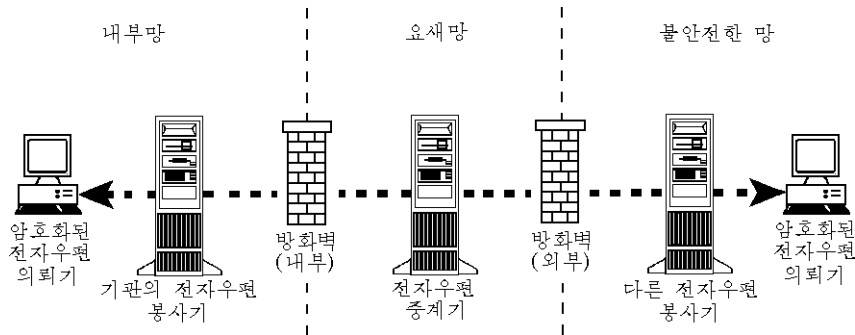



그림 13－2. 암호화

그러나 이 방법과 관련하여 다음과 같은 많은 문제점들이 있다.

- 암호화는 오직 송신자가 암호화특징을 리용하여야 하겠다는것을 생각하였을 때에만 진행될수 있다.
- 각이한 기관의 사용자들이 같은 암호화체계(S/MIME, PGP 등)를 리용하는데 동의하여야 한다.
- 매 말단의 사용자와 의뢰기의 쏘프트웨어는 사용할 암호화열쇠들에 대한 정보를 교환할수 있어야 한다.

같은 기관 혹은 관련된 기관들이 지리적으로 떨어 져 있는 사무실들사이의 망접속을 제공하기 위한 목적에 인터네트가 리용되는 경우에도 암호화된 VPN은 기관내부전송에 필요한 보호를 제공할수 있다. 그때에는 단순히 싸이트들사이 전자우편전송의 경로조정을 VPN을 통하여 진행하도록 할 필요가 있다.

두 영업동료들사이의 통신은 암호화에 의한 보호를 요구하지만 어떤 원인으로 VPN을 실행할수 없는 경우에는 우편암호화장치가 그림 13－3에 보여 준바와 같이 내부우편봉사기와 불안전망사이에 설치될수 있다. 그 장치는 일단 설치되면 특정하게 설정된 싸이트들과 교환되는 전송흐름에 대하여서는 암호화/복호화하도록 설정되지만 그렇지 않은 싸이트들에 대하여서는 암호화되지 않은채로 통과하도록 한다.

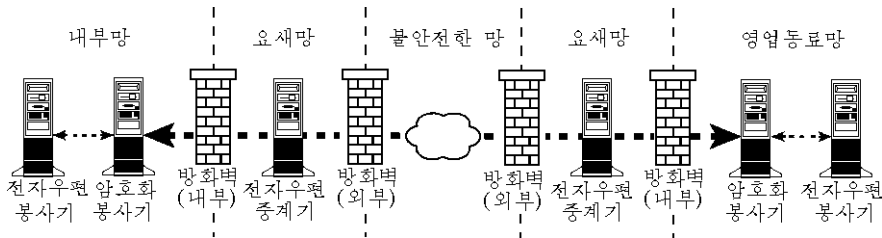



그림 13－3. 우편암호화장치설치

봉사기들사이를 통과하는 통보문뿐아니라 봉사기들과 사용자워크스테이션들사이를 통과하는 전송흐름의 보안도 고찰할 필요가 있다. 대부분의 전자우편응용쏘프트체계는 의뢰기와 봉사기쏘프트웨어사이 통신통로를 암호화할수 있는 능력을 가지고 있다. 암호화의 적용은 봉사기환경에서 부하를 상당히 증가시키므로 일반적으로 기정값은 미사용(disabled)으로 한다. 일부 체계들은 다른 체계들이 SSL/TLS와 같은 현존 암호화표준을 리용하는것과는 달리 독자적인 암호화체계를 리용한다.

사용자들이 집에서 혹은 려행하면서 전자우편을 사용할 때 접속보안에 특별한 주의를 돌려야 한다. 일부 큰 기관들은 경제적견지에서 자체의 안전원격접근체계를 내부망자원에 제공할수 있지만 원격사용자들의 접속을 위해서는 더욱더 인터네트를 리용하는 방향으로 나가고 있다. 리용되는 모든 접근방법들(전용방법, SMTP, POP, IMAP, Web메일 등)은 이 암호화를 계획할 때 고려할 필요가 있다.

원격사용자들은 봉사기에로 통신할 때 전자우편의뢰기를 암호화하는 대신 암호화가능원격접근봉사기를 리용할수 있다(그림 13－4 참고).

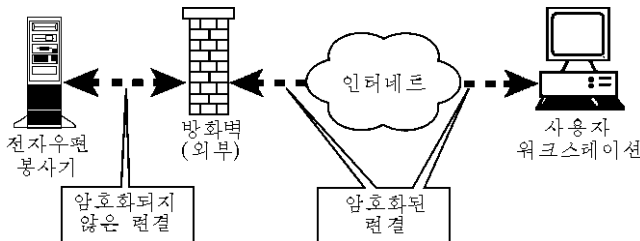



그림 13－4. 암호화가능한 원격접근봉사기

이 장치들은 사용자들의 워크스테이션에 설치된 쏘프트웨어에 암호화된 턴넬을 직접 형성하기 위하여 전문적으로 사용된다. 원격워크스테이션들에 VPN턴넬을 형성하는데는

원격접근봉사기들의 첨부, 의뢰기워크스테이션상에 VPN쏘프트의 설치 및 설정, VPN턴넬설치에 사용되는 인증체계의 유지 등이 요구된다. 그러나 일단 설치되면 원격사용자들이 임의의 내부망자원에 접근할수 있도록 보다 많은 전자우편접속을 제공한다.

인터네트에서 전송흐름(traffic)의 교환에 리용되는 전자우편규약은 SMTP(Simple Mail Transfer Protocol)라는것이다. 1982년에 처음으로 개발된 이 규약은 실행하기가 특별히 쉬웠으며(그때) 단순한 인터네트(거의 학술적으로 리용)상에서 사용될것을 목적으로 하였다. 몇년동안 쓸모 있는 기본규약으로 많은 확장과 갱신을 하였지만 초기설계의 유산은 많은 보안문제들을 산생시켰다.

초기에는 SMTP통보문발신자의 인증을 결정할수 있는 어떠한 구조도 가지고 있지 못하였다. 많은 체계들에서 해당한 통보문의 발신자마당에는 사용자가 자기의뢰기쏘프트웨어에 입력해 넣는것이 들어 간다. 만일 사용자가 syn_kos@university.edu.kp이라고 입력하면 그것은 자기 의뢰기쏘프트웨어의 발신자마당에 들어 간다. 만일 의뢰기체계로부터 통보문을 받는 봉사기가 발신자신원을 거절하지 않으면 그것은 중계 및 배포처리를 하는 동안 임의의 다른 곳에서도 거부되지 않을것이다. 봉사기쏘프트웨어는 다음과 같이 설정되여야 한다.

- 국부사용자로부터 접속이 수립되는 동안 제출된 통보문의 발신주소가 인증된 신원과 맞는가를 요구하여야 한다. 그러나 유감스럽게도 대부분의 열린체계들은 기정값이 그렇게 설정되여 있지 않으며 일부는 그렇게 하기가 완전히 불가능하다. 독점체계들(Microsoft Exchange, Lotus Notes Domino 등)은 전용제출방식(MAPI 등)을 사용할 때에는 사용자인증을 위하여 전형적으로 정확한 발신자전자우편주소를 요구하지만 접속에 열린표준의뢰기(SMTP/POP/IMAP)들을 허락할 때에는 그렇게 하지 않는다.
- 통보문의 발신자주소가 국부사용자를 나타낸다면 대화인증을 요구하여야 한다. 그렇게 하도록 주의를 돌려 설정하지 않으면 SMTP를 통하여 통보문을 받는 대부분의 체계들은 이 검사를 진행하지 않는다.

이 문제들에 대한 방도는 ASMTP(Authenticated SMTP)를 사용하는것이며 일단 인증된 사용자는 자기 주소가 아닌 다른 발신주소를 가진 통보문을 제출하지 않도록 하는것이다(한 사용자가 다른 주소를 가질수 있다고 가정하는것은 위험하다.).

미리 이야기할것은 특정IP주소(대표적으로는 인증할수 없는 전자우편전송을 발생하는 응용프로그람봉사기)에 대해서는 ASMTP요구를 무시할 필요가 있다는것이다. 이런 경우에 그런 전자우편전송을 시도하는 봉사기의 IP주소는 《인증》되여야 한다.

ASMTP는 기관의 령역안에서 통보문의 모조를 막는데 사용할수 있지만 외부기관으로부터 접수하는 통보문의 타당성검사에는 사용할수 없다. 일반적으로 최선의 방도는 어떤 봉사기에로 통보문전송을 시도하는 봉사기의 IP주소나 호스트이름이 그 통보문의 발신자주소의 령역에 《적합》하도록 하는것이다. 이렇게 하지 않고 기관들사이의 동의가 없이 들어 오는 통보문의 타당성을 평가하려는 어떠한 시도도 억측에 불과하다.

이 문제에 대하여 가장 쓸모 있는 하나의 해결책은 사용자들에게 이러한 정황을 가

르쳐 주고 외부령역으로부터 들어 오는 모든 전자우편통보문들을 옳게 평가하는것이다. 모든 내부전자우편이 인증을 요구한다고 해도 신용증(대표적으로 사용자이름/통과암호결합)들은 추측되거나 도난 당하거나 아니면 신용성이 떨어 진다(전자우편사용에서 사용자의 적합한 훈련은 이하의 여러 부분들에서도 취급된다.).

《열린중계기》라는 조건을 방지하도록 해당 우편봉사기를 설정하는것이 또한 중요하다. 열린중계기의 기능을 수행하는 우편봉사기는 어떤 발신자주소를 가지는 통보문을 어떤 수신자주소에로 배포하기 위하여 받아 들일것이다. 인터네트의 력사적관점으로부터 고찰해 볼 때 열린중계기는 다른 기관의 통보문을 발송해 주는 훌륭한 우편배달부였다. 현대적시점에서 열린중계기는《스패머(spammer)들》의 동작을 허용하는 믿을수 없는 나쁜 배달부로 볼수 있다. 검사를 하지 않은채로 계속 내버려 두면 해당 기관의 우편봉사기들은 《검은 명단에 올려 지게》 되고 다른 많은 기관들과 통신할 수 없게 된다(이것은 더 정확하게는 비요청전자우편다량배포(UBE—Unsolicited Bulk E-mail)로 알려 져 있는데 이 장의 썩 뒤에 《스팸(spam)》이라는 내용에 서술되여 있다.).

보안의 견지에서 다음과 같은 세가지 기본견해가 있다.

- 스패머들은 허가나 보상도 없이 또는 간단히 《봉사를 훔쳐서》 어떤 기관의 처리능력과 접속대역너비를 리용할수 있다.
- 만일 이런 사용을 검사하지 않은채로 방임하면 그 기관의 전자우편체계와 대역너비가 그 기관의 전자우편사용을 저하시키거나 전혀 사용불가능하도록 하는데 악용될것이다.
- 자기의 체계가 전송흐름을 처리하도록 허용하는것은 자기 기관의 영상을 떨어뜨리고 대외관계에 손상을 줄수 있다.
- 자기 우편봉사기가 중계기로서 동작하던것을 《종결》시키려면 다음과 같은 두가지 기본조건에서만 전송흐름을 접수하도록 설정되여야 한다.
  - 통보문을 제출하려고 시도하는 어떤 다른 체계도 자기 체계의 사용자로서 정확히 인증이 되였으며 그 통보문의 발신주소는 인증된 신원(ID)과 일치한다(그러나 빈 우편주소 “< >”는 수신 및 배포통지 등에 리용될 때 임의의 신원에도 유효하다.).
  - 통보문을 제출하려고 시도하는 체계는 사용자로서 인증되지 않고 발신주소는 외부령역으로부터 오며 통보문의 모든 수신자는 기관령역내부에 있다.

중계능력을 차단하기 위하여 제작자가 권고한대로 전자우편체계를 설정할뿐아니라 권고된 설정이 실지로 중계를 차단하도록 설정된후에 봉사기의 중계상태를 검사하는것이 중요하다(현재 권고안대로 설정했을 때 여전히 부분적으로 열리는 여러가지 중요전자우편중계기제품들이 상품화되고 있다. 중계차단에 필요한 설정에 대한 최신정보를 얻을수 있는 가장 좋은 방법은 MAPS, ORBS, CAUCE와 같은 여러 스팸대응(anti–spam)회사들로부터 쓸모 있는 직결봉사를 받는것이다.).

전자우편내용에서의 위험과 문제점

확실히 전자우편보안에서 가장 심각한 문제의 하나는 비루스의 전파일것이다. 전자우편이 광범히 보급되기 이전에 콤퓨터비루스는 몇주, 몇달 혹은 몇년에 한번씩 빈번히 나타나 널리 만연되였다. 최근에는 많은 전자우편의뢰기들의 일정한 자동특성과 일부 비루스범죄자들에 의한 다소 교묘한 《사회공학》의 덕택으로 여러가지 최신비루스들이 하루가 멀다하게 널리 류포되였으며 대규모전자우편체계들을 순간에 무너뜨렸다. 전자우편체계를 통한 비루스의 류포를 방지하는것은 명백히 매우 우선시할뿐아니라 주의를 돌려 계획하고 수행할것을 요구한다(트로이목마와 같이 기술적으로 비루스가 아닌 다른 프로그람들과 스크립트들도 이 부류에 속한다.).

전통적으로 비루스방지는 모든 워크스테이션에 항비루스쏘프트웨어를 설치하는것을 통하여 진행되였다. 이것도 물론 여전히 중요하지만 그것만으로는 현재의 모든 형태의 전자우편비루스들을 다 방지할수 없다. 특히 많은 전자우편의뢰기쏘프트웨어패키지들은 내부스크립트처리 및 실행환경을 가지고 있다(JavaStet, VBS 등). 여러 종류의 비루스들은 전통적인 항비루스쏘프트웨어의 개입을 막는 방법으로 전자우편령역내부의 바로 이 기능을 악용하였다. 그런 비루스의 첫째가는 큰 규모의 실례는 “ILoveYou”비루스이다. 솜씨 있는 프로그람작성과 사회공학의 결합을 통하여 이 비루스는 전자우편의뢰기들이 국부사용자의 모든 주소목록의 입구에 자기의 복사본을 보내도록 시동하였다. 발생되는 전자우편의 용량은 봉사거부공격이 산생되는 수준에까지 이르러 간접적으로 많은 전자우편봉사기들을 마비시켰다.

전자우편비루스들을 제거하기 위한 다른 하나의 전통적인 방법은 내부전자우편체계와 인터네트사이에 비루스검사중계기를 배치하는것이였다. 이것은 비루스공격으로부터 전자우편체계를 보호하기 위한 계층화된 방어에서 여전히 중요한 단계로 되는데 그것은 여러 봉사기전자우편의뢰기에 받아 들이기 쉽다. 대부분의 전자우편의뢰기들 특히 열린 표준들(SMTP/IMAP/POP)에 대하여 설계된 전자우편의뢰기들은 여러 봉사기상의 여러 구좌들이 호상작용할수 있게 설계된다. 사용자들은 자기의 의뢰기가 기관구좌와 하나 혹은 그이상의 개인구좌(home ISP, 동우회, 동창생 등)들과 다 호상작용하도록 이 특성을 자주 리용한다. 의뢰기는 원격봉사기들에 접근하는데 IMAP 혹은 POP을 리용하기때문에 항비루스기능을 가진 SMTP중계기는 이 트랜잭션(transaction)들을 보호할수 없다. 일단 비루스에 감염된 통보문이 사용자의 워크스테이션에 도달하면 그때에는 내부망안에서 자유롭게 복제될수 있다.

이 가능성을 피하는데는 다음과 같은 두가지 방법이 있다.

첫째로, IMAP와 POP의 TCP포구들을 차단하며 외부 전자우편봉사기로부터 내부망의 봉사기들을 보호하는데 방화벽을 설정할수 있다. 이것은 무릎형콤퓨터나 다른 휴대형콤퓨터장치들로 하여 효과성이 제한된다(사용자는 무릎형콤퓨터를 집에 놓고 자기의 ISP접속을 통하여 보호되지 않은 우편봉사기들에 접근한다. 만일 비루스에 감염된 통보문을 받았다면 후에 다시 무릎형콤퓨터를 사무실에 가져 가서 내부망에 접속하였을 때 비루스가 동작할수 있다.).

둘째로, 전자우편봉사기와 함께 직접 동작할수 있게 설계된 항비루스쏘프트웨어를 모든 내부봉사기에 설치하는것이다. 이 쏘프트웨어는 통보문이 내부망에 도달하였다 하더라도 전자우편비루스의 류포를 방지하면서 제출되는 모든 통보문들을 주사한다(이 쏘프트웨어는 전자우편특정비루스만이 아니라 모든 비루스형태를 다 주사한다.).

전자우편비루스의 류포속도와 관련하여(ILoveYou비루스는 하루도 못되는 사이에 전세계에 류포되였으며 일부 전자우편봉사기들을 마비시키였다.) 새로운 항비루스정의와 함께 거의 실시간적으로 그리고 좋기는 자동적으로 갱신될수 있는 항비루스프로그람을 입수해야 할 필요가 있다. 항비루스해결책을 평가하는데서 전자우편봉사기들과 중계기들을 위한 항비루스체계는 빨리 갱신될수 있게 하는것이 가장 중요하다. 가능하면 항비루스해결방안 판매업체들이 봉사기들에 새로운 비루스정의를 전송하여 자동적으로 갱신되는 봉사기항비루스해결방안을 선택하는것이 좋다(주요 신판비루스의 공격후에 즉시 판매업체싸이트들로부터 갱신판을 내리적재하려는것은 문제가 있을수 있다.).

비루스방지를 제공하는 가장 좋은 방법은 아래와 같은 계층방식이다.

- 워크스테이션들은 항비루스체계를 설치하고 적합하게 갱신하여야 한다. 이 프로그람들은 일부 전자우편특정비루스들을 방지하지 못할수도 있으나 다른 비루스전파방법들로부터는 보호하며(휴대형매체, 공유된 보관소를 통한 전송 등) 주요형태의 파손을 방지한다(디스크의 초기화, 파일삭제 등).
- 내부망안에 있는 전자우편봉사기들은 원격전자우편구좌에 접근하는 휴대형콤퓨터 및 의뢰기들로 인하여 내부망들에 들어 오는 비루스들로부터 이 봉사기들을 보호하기 위하여 모든 전자우편통보문들(모든 첨부파일들 포함)을 주사하도록 설계된 항비루스쏘프트웨어를 가지고 있어야 한다. 이 쏘프트웨어는 거의 실시간적으로 최신비루스정의들로 유지보존되여야 한다.
- 내부망과 인터네트(혹은 비신뢰망)사이에 전송흐름을 통과시키는 전자우편중계기들은 내부체계들과 비신뢰외부체계들사이의 비루스전염을 조종하기 위한 항비루스체계들을 가지고 있어야 한다. 이 체계는 거의 실시간적으로 최신항비루스정의들로 유지갱신되는것이 아주 중요하다. 인터네트상의 비루스전염《폭풍》이 일어 나는 곳들에서 이 체계는 내부전자우편봉사기들이 들어 오는 비루스감염된 통보문들을 처리(거절 또는 처치)하느라 쩔쩔 매는것을 막을것이다(중계기체계는 마비되지만 기관내부의 전자우편은 실시가능한채로 있다.).
- 내부사용자들이 사용하는 전자우편의뢰기쏘프트웨어는 자률적인 비루스전염을 막게끔 최대한의 보안설정이 되여야 하며 판매업체로부터 제공되는 유용한 최신보안보강대책으로 유지되여야 한다. 많은 경우 설치시의 기정설정은 아주 불안전하다.
- 전자우편사용자들은 여러 형태의 전자우편비루스들과 전자우편을 사용할 때 취하여야 할 예방조치들에 숙련되여야 한다. 이것은 트로이목마프로그람들의 전염을 막는데서 특별히 중요하다(알지 못하거나 믿을수 없는 원천들로부터 전자우편의 부착물을 절대로 열어 보지 말것. 알려 진 원천으로부터 오는 예견치 않은 전자우편부착물을 의심할것. 의심스러운 통보문을 받게 되면 어떤 방조를 받겠

는지 알고 있을것.)

다른 하나의 비기술적인 형태의 비루스가 있는데 그것은 속임(hoax)비루스이다. 이 비루스들은 전형적으로 전자우편을 통하여 류포되는 아주 새로운 비루스에 대한 상세한 내용으로 이루어 져 있다. 비루스에 대한 서술내용은 완전히 거짓일수 있는데 서술내용은 접수자가 공포에 빠지도록 아주 정교하게 만들어 지며 독자로 하여금 말을 퍼뜨리게끔 한다. 이런 여러가지 속임비루스 경고문들은 아주 설득력 있어서 수많은 사용자들이 수많은 수신자들에게 그 통보문을 전송하도록 한다. 결과적으로 전자우편체계는 이 통보문들의 용량으로 하여 과부하를 받게 되며 매우 유력한 봉사거부공격이 산생된다. 사용자들은 이러한 정황에 대처할수 있는 다음과 같은 방법들을 알고 있는것이 중요하다.

- 그러한 비루스경고들을 여러 수신자들에게 전파시키지 말라. 요컨대 위험정도를 평가할수 있는 기관내의 책임적인 당사자에게 단일복사본을 전송하도록 사용자들에게 알려 주라(만일 그것이 진짜 위협으로 된다면 그사람 또는 기관은 그 통지에 대하여 자기의 의무를 리행하게 된다.).
- 사용자는 기관내의 특정주소에서 오는 진짜 비루스위협경고를 접수할 용의가 있으며 그러한 통보문만을 신뢰한다.

사용자는 비루스에 감염된 통보문과 비루스경고문처리뿐아니라 전자우편의 여러가지 측면에도 훈련되여야 한다. 앞에서 서술한 권고들은 위조전자우편(보통 spoofing)들을 막는데 도움이 되였다. 대표적인 사용자들은 보통 그것이 얼마나 간단히 전자우편을 위조할수 있는지 모른다. 사용자들은 자기가 접수하는 모든것에 대하여 맹목적으로 믿지 않도록 훈련되여야 한다. 만일 밖에서 어떤 방법으로 보통 습관과 절차에 따르는 전자우편을 받았다면 그 내용은 다른 통로를 통하여 확인할 필요가 있다. 사용자들이 전자우편의 타당성을 맹목적으로 믿음으로 하여 일련의 문제가 생겼다. 일부 실제한 실례들은 깜짝 놀랄 정도이다.

- 지나친 장난이 동료에 의하여 저질러 졌다. 어느 한 종업원은 자기 지배인으로부터 《당신은 해고되였소. 당신의 개인소지품들을 책상과 사무실에서 걷어 가지고 저녁 5시까지 회사밖으로 나가시오.》라는 전자우편을 받는다. 또 다른 경우로는 한 종업원의 책임자인듯 한 사람으로부터 회사의 보안부서에 그 종업원이 사무실비품들을 훔쳐 간다는 거짓전자우편이 온다.
- 불평 많은 종업원이 말썽을 일으킨다. 그는 재정담당부사장으로 가장하고 주문담당자에게 지불을 제대로 하지 않으므로 다시 통지가 있을 때까지 한 주요고객에게 보낼 주문품납입을 중지하라는 전자우편을 보낸다.
- 정직하지 못한 사람(기관밖의)은 고위 판매담당부사장이 보내는것처럼 전자우편을 위조한다. 그 전자우편은 앞으로 있게 될 무역전시회에 예견된 고객들에게 보여 줄 견본으로 될수 있게 100대의 제품견본을 다른 나라의 어떤 주소로 보낼것을 지시한다. 부주의로 하여 보통의 문서놀음에 따라 그 견본들은 즉시 발송

되게 된다.

지배인이 전자우편을 통하여 실지로 종업원을 해고하겠는가. 이 지시나 주문들이 전자우편으로 정상적으로 통신되는가, 사용자들은 어떤 문제들이 전자우편을 통하여 일상적으로 처리되며 언제 어떻게 그런 통보문들을 문의하거나 확인할것인가를 알려 줄것을 요구한다. 만일 통보문의 접수자가 이런 형태의 통보문을 맹목적으로 받으면 비참한 결과를 초래할수 있다.

전자우편통보문들은 거의 실시간적으로 이동하며 대부분의 전자우편체계들은 보관 및 기록능력을 극히 제한하므로 체계와 절차들은 계속 진보되고 조사될것을 요구한다. 앞에서는 장난, 파괴행위, 절도 등의 불쾌한 행위들에 대한 실례를 들었다. 그외에도 전자우편을 통하여 진행되는 산업정탐, 성희롱, 위협, 불법거래 등의 문제들이 있다.

대부분의 주요회사들은 적극적인 준법활동을 벌려 사용자들로 하여금 정확히 행동하고 리용하도록 가르쳐 주고 있으나 그런 문제들은 아직 계속 조사되여야 한다. 독자는 사적비밀, 자료보전, 암호화에 관한 법의 테두리내에서 다음의 정보들이 고려되여야 한다는것을 알아야 한다.

방책과 절차는 최소한 《적합한》기간 전자우편체계의 기록을 보전하도록 수립되여야 한다. 임의의 전자우편체계는 정상적으로 매 통보문의 발신자, 수신자, 크기, 접수 및 배포시간 등을 기록한다. 많은 전자우편봉사기들은 기록되는 정보의 량과 형태를 조종하는 선택적인 기록설정들을 가진다. 가능한껏 다음의 설정들이 조사를 요구하는 가장 신중한 정보를 기록하기 위하여 시험되고 설정되여야 한다.

- 임의의 통보문에 대한 실제적인 발신원천의 지적(“From”마당과 관계없이)한다. 가능하면 인증된 사용자를 포함한다. 통보문을 제출하는 워크스테이션이나 봉사기의 이름이나 망주소는 교차적인 지적이나 발신자인증을 확증하는 자료로서 중요하다. 만일 통보문을 보내는 콤퓨터사용자가 여럿이라면 통보문전송에 어떤 구좌가 리용되는가.
- 통보문에서 기본내용 혹은 다른 머리부들은 개별적통보문들을 식별하는데서 그리고 여러 전자우편봉사기와 체계들을 통과하는 경로설정에서 결정적이다.
- 부착물의 내용류형과 이름(례: customers.doc ─ 응용프로그람/ms–word, ”nudie.jpeg” ─화상/jpeg 등)도 도움이 된다.

또한 일부 전자우편체계들은 여벌의 통보문들을 복사해 두도록 한다. 이 복사본들은 가능하면 완전한 내용을 보존한다. 일부 체계들은 체계를 통하여 전송되는 모든 통보문들을 기록해 두는가 하면 다른 일부 체계들은 발신자/수신자주소 또는 령역, 우선권, 크기 또는 다른 요인에 따라 어느 통보문을 보관할것인가를 나타내는 조종인자들을 가지고 있다. 만일 보관특성이 유용하다면 전자우편체계들에 보충적인 큰 보관장소를 분배하며 따라서 기관적인 요구, 우선권, 예산들을 결정하고 잠재적인 보안요구와 균형을 맞추는것이 필요할것이다.

보관특성이 유용하지 못한 체계들의 경우에는 통보문의 복사를 허용함으로써 자동적

으로 생성되여 접수자에게 전달(계획하지 않은)되도록 한다(대표적으로 이것은 bcc 또는 auto–forward 특성들이다.). 이 특성들은 모든 사용자들에게 사용될수 있을만큼 효과적인것이 못되며 따라서 그것들은 일반적으로 새로운 조사에만 유용하다.

만일 조사가 요구되면 봉사기기록이나 기록된 통보문들을 검색하는데 효과적인 검색 또는 보고도구가 없이 수집된 정보를 통하여 엄밀한 조사를 진행하는것은 불가능하다. 이미전에 나온 필요한 도구들을 습득하고 조사하는것이 제일 현명하다. 도구들의 기능은 검증되여야 하며 결국 그 도구들과 친숙해 지면 귀중한 시간을 절약할수 있을것이다.

일부 기관들에서는 전자우편의 개인적사용이 종업원의 특전이외의 다른 아무것으로도 되지 않는다. 만일 기관의 방책이 전자우편의 사용을 공적인 사업에 국한시킨다면 개인적인 사용은 봉사의 도난으로 간주된다. 이런 경우 사용자들의 사용방식(동료와의 사업상 련관이 없는 전자서신거래 즉 오락, 체육, 롱담목록들로부터 통보문을 받는것)이나 내용의 류형(다매체－화상, 비데오, 오디오, 게임 등)들을 탐지하여야 할 필요성이 제기된다. 그러나 전자우편봉사기체계는 전형적으로 기능성과 융통성이 있게 설계되지 내용을 제한하게끔 설계되지는 않는다. 사용방식을 감시하는 능력은 전적으로 봉사기기록파일의 우편처리에 국한된다. 내용류형에 따르는 전송흐름의 감시, 려과, 기록 또는 보존능력은 리용할수 없다.

이런 특성들을 제공하기 위하여 설계되는 전자우편중계제품 및 봉사는 쓸모 있다. 일반적으로 전자우편방화벽이라는것은 보통의 방화벽이 망계층인것과는 반대로 그 과정이 응용프로그람계층에서 진행되는것이다(그것이 전형적으로 제공하는 여러가지 특성들은 이 장의 뒤부분에서 설명한다.). 이 전자우편방화벽들이 사용되는 경우 여러 측면에서 효과적일수 있지만 일반적으로 그것들은 봉사기사이를 통과하는 통보문들에 국한되며 전형적으로 내부전자우편체계와 인터네트사이의 경계에 설치된다. 같은 봉사기의 각이한 사용자들사이에 오가는 통보문들은 전적으로 내적으로 처리되며 이 장치들에 의하여 조사될수 없다.

무 선 보 안

전자우편접속에서 제일 최근에 새롭게 개발된것은 무선자료통신이다.《무선》이라는 말이 하나의 단일한 범주로 자주 론의되고 있지만 여러가지 장치들이 각이한 방법으로 각이한 형태의 자료망들에서 인터네트에 호상접속을 위한 여러 기술들과 함께 동작한다. 주되는 보안우려는 전자우편자료가 전송도중에 무선련결상에서든 인터네트련결상에서든 중간에서 도청 당할수 있다는것이다. 휴대형호출기를 제외하고 대부분의 무선자료장치들은 무선련결시에 일정한 형태의 암호화를 한다. 봉사의 형태가 아주 다양하고 시장의 변화가 빠르므로 해당한 특정봉사를 검사하는것이 필요할것이다. 이 모든 장치들은 일부 통보문경로조정에 대하여 인터네트를 리용하는데 이 경로조정부분은 고유한 의미에서 암호화를 지원하지 않는다.

현재의 무선장치들중에서 손 꼽히는것들은 이동전화, 인터네트모뎀, PDA, LAN기판,

휴대형호출기 등이다.

수자식이동전화 망기술의 특성들이 다양하지만 이 장치들은 모두 초기에 수자식으로 부호화된 두방향음성전화호출신호를 전달할수 있게끔 설계된 망들을 리용한다. 자료망을 리용할 때 일단 신호가 무선전화탑에 도착하면 인터네트와 호상 접속하기 위하여 여러가지 방법들이 리용된다. 전자우편봉사는 다음과 같은 두가지 방법으로 전화에 제공된다.

- 첫째로, 이동전화는 HTML이나 WAPWeb우편을 통하여 전자우편에 접근할수 있다. 이 접근방식은 이 Web접근이 접속할 때 SSL암호화를 지원하지 않는다는것을 제외한다면 보통의 인터네트접근과 기능적으로 같다.
- 둘째로, 일부 무선전화봉사제공업체들은 전화에 하나의 전자우편구좌를 제공한다. 이 경우에 무선전화제공업체는 전자우편봉사기로 동작한다. 보통 이것은 이 장치를 가진 사용자들이 일부 또는 모든 전자우편을 자기들의 국부구좌로부터 이동전화구좌로 자동전송하도록 설정하려 할수 있다는 가능성을 제외한다면 기관의 전자우편보안과 관계없다. 자동전송되는 통보문들은 인터네트로 암호화되지 않은채로 전송된다는것을 명심하여야 한다.

무릎형콤퓨터 및 PDA(WAN)용무선인터네트모뎀, 무선모뎀내장 PDA, PDA통합수자식이동전화 이 장치들은 독립적인 무선망이나 수자식이동전화망을 다 리용할수 있다. 일단 자료가 인터네트상으로 무선망을 통하여 지나가면 자료는 암호화되지 않는다. 무릎형콤퓨터는 접속에 우선 암호화를 리용하여 이 문제를 극복할수 있지만 PDA용의뢰기쏘프트웨어는 흔히 SSL암호화를 할수 없다.

무선LAN카드 여러가지 각이한 기술을 리용하는 이 장치들의 종류는 다양하다. 판매업체들의 문서에는 통보문이 암호화되여야 하는가 그리고 련결할 때 암호화가 가능 혹은 실행으로 설정되여야 하는가 하는것이 밝혀 져 있어야 한다.

무선전자우편특정장치 일부 다른 기능들이 특이하게 포함되여 있지만 기본기능은 전자우편통보문들을 주고받을수 있는것인데 암호화된 무선자료망이나 암호화되지 않은 휴대형소형무선호출망을 리용할수 있다. 이 장치들은 모두 무선장치와 봉사제공업체간의 통신에 전용규약들을 사용한다. 그것들은 다음과 같은 두가지 방식으로 동작한다.

- 첫째로, 봉사제공자는 장치의 전용규약과 열린표준규약들(CMTP/POP/ IMAP)사이에서 미리 설정된 전자우편호스트에로 중계하는 관문을 제공할수 있다. 봉사는 인터네트접속에 SSL을 지원할수 있고 지원하지 않을수도 있으며 ASMTP를 통하여 통보문을 제출하는 기능을 가지고 있을수도 있고 그렇지 않을수도 있다.
- 둘째로, 봉사제공자에 의하여 동작하는 하나의 전자우편봉사기상의 장치에 봉사제공자는 별도의 전자우편구좌를 제공할수 있다. 또한 한 기관내의 사용자들은 자기의 일부 또는 모든 전자우편을 이 구좌에로 자동전송하려고 할수도 있다. 그러면 자동전송되는 우편은 인터네트에서 이 구좌의 봉사기에로 암호화되지 않은채로 이동할것이다.

문자수자휴대형호출기와 두방향휴대형호출기 이 장치들을 위하여 봉사제공업체는 휴대형호출기와 관련된 전자우편주소를 제공한다. 봉사제공업체의 봉사기가 그 주소에 대한 전자우편을 받으면 통보문은 표준적으로 최소본문형태로 분해되여 휴대형호출기로 전송된다. 무선통신은 전형적으로 암호화되지는 않는다. 두방향휴대형호출기는 보통 단순한 중계통보문을 보내는 방식을 취한다.

하나의 전자우편구좌가 봉사제공업체의 전자우편봉사기로 발송될것을 필요로 하는 접근방식을 사용하는 이 장치들에 대하여 인터네트상에서 정보가 암호화되지 않고 전송되므로 신중한 정보는 자동전송되지 않도록 주의를 돌려야 한다. 만일 자동전송이 충분히 선택적으로 설정될수 없다면 인터네트에로의 자동전송을 허락하지 말아야 한다.

인터네트를 통하여 기관의 전자우편봉사기에 접근하는 무선장치와 SSL대화암호화보호가 리용되지 않는 경우 접근을 막을것인가 혹은 사용자가 인터네트로부터 전자우편봉사기에 원격으로 접근하지 않는다고 믿을것인가 하는것을 결정하는것이 필요하다.

전자우편보안도구들

이 론문을 작성할 때(2001년 초)에는 전자우편보안에 직접 적용할수 있는 기본적으로 다음과 같은 세 부류의 도구들이 있었다.

전자우편암호화체계들 이 장치들은 설정된 전자우편봉사기들사이의 전송흐름을 암호화 및 복호화하는 전자우편중계장치형태로서 흔히 쓸모 있다. 현재 대부분은 여러가지 경쟁적인 전자우편암호화표준가운데서 하나(기본적으로 S/MIMF과 PGP)를 리용하지만 일부는 전용암호화체계를 사용한다.

이 장치들은 잘 채용되지 않고 전자우편암호화에 대한 명백한 단일표준이 없으며 PKI기반에 여러가지 문제가 있음으로 하여 보통 일반적인 체계들사이나 혹은 협동기관들사이에서만 쓸수 있다.

전자우편운용호환성을 가진 항비루스체계 전자우편봉사기와 봉사기판매업체들은 항비루스방지의 필요성을 인정하기는 하였으나 일반적으로 항비루스계에 능란하지는 못하다. 대부분의 경우 봉사기쏘프트웨어제조업체들은 통보문처리의 접수와 배포단계사이에 통보문처리를 위한 API를 제공하는데 그 봉사기쏘프트웨어제조업체들중 하나 혹은 그이상의 항비루스판매업체들이 봉사기특정제품들을 많이 제공한다. 또한 열린표준(SMTP)체계들의 통보문접수규약을 즉시 받아 들이도록 설계된 일부 전자우편항비루스봉사기제품들도 있다.

전자우편방화벽제품과 봉사 전자우편방화벽제품과 봉사는 다 항비루스, 반스팸(anti–spam), 내용려과(내용탐색), 내용류형려과(첨부품이름이나 형태탐지), 통보문보관, 사용방식보고, 우편접수거부자공시 , 봉사거부공격에 대처한 적재제한, 암호화, 위조대응(anti–counterfeiting), 위장대응(anti–spoofing), 사용자감시 등을 포함하는 많은 결합기능들을 가질수 있다.

암호화나 방화벽제품 또는 봉사를 리용하도록 설계하면 그것이 적용된 전자우편봉사

기들사이에 어떻게 위치하겠는가를 평가하는것이 또한 필요하다. 단 하나의 봉사기만을 가지는 기관들에서는 전자우편봉사기와 인터네트사이에 중계기로 배치될수 있다. 만일 기관이 보호되여야 할 여러개의 봉사기들을 가지고 있을 때 전자우편경로조정에 방해를 주지 않으면서 여러개의 봉사기들에 봉사를 제공하기 위하여서는 그것이 어떻게 배치되여야 하는가를 결정하는것이 중요할것이다.

최신으로 갱신

전자통신환경은 일반적으로 급속히 변한다. 매 판매업체들은 몇달에 한번씩 보안에 영향을 줄수 있는 새로운 특징들이 있는 새로운 봉사기 및 의뢰기쏘프트웨어들을 내놓는다. 해커들과 보안전문가들은 정상적으로 현존 제품들의 우점과 약점들을 발견해 내며 판매업체들은 그 결함들을 극복한 보강프로그람(patch)들과 새로운 개정판들을 만들어 낸다. 한편 새로운 비루스들을 적극적으로 만들어 내는 자들도 숨어 있다. 이런 개발을 유지하려는 개별적사람들은 그 분야에 대한 자기의 지식을 정상적으로 갱신할 필요가 있다.

최신의 보안과 비루스문제들에 대한 가장 좋은 정보원천은 일반적으로 인터네트의 Web싸이트 및 메일링리스트들에서 찾아 볼수 있다(물론 써퍼(surfer)들도 그 원천을 평가하는것이 중요하다.). 중요한것은 다음과 같다.

- 콤퓨터비상대응팀(CERT:Computer Emergency Response Team): 일반적인 콤퓨터보안문제들에 대하여 CERT는 정기적으로 전자우편 및 비루스와 관련된것들을 포함하여 블레찐을 발행한다.
- 전자우편봉사기 및 의뢰기쏘프트웨어판매업체들은 보안문제들에 대한 정보의 중요한 원천이다.
- 기본(rootshell)Web싸이트는 봉사를 방해할수 있는 공격들에 대한 중요한 정보를 정기적으로 제공한다.

항비루스쏘프트웨어의 판매업체들은 새로운 비루스들에 대한 시기적절한 정보를 주는 좋은 원천들이다. 자기의 판매업체를 확인해보라. 많은 판매업체들은 자기의 Web싸이트에 접근할수 있는 권한을 제한하거나 자기의 고객에 한해서만 메일링리스트를 제공해준다.

요 약

이 장에서는 기관환경에서 사용할 때 부닥치는 전자우편과 보안문제의 일반적인 견해를 주는데 초점을 두었다. 전자통신의 력사적측면으로부터 시작하여 본문에서는 수많은 전자우편위험요소들을 조사하고 그 리면에 기술적이며 조작상의 개념들을 상

세히 서술하였으며 IT기관들이 그것을 제거하는데 리용할수 있는 도구와 응용프로그람들을 보여 주었다. 또한 본문에서는 기관에서 무선보안을 실시하기 위한 전략을 제공하였다.

용 어 해 설

ARPAnet(Advanced Research Projects Agency NET work)

선진연구계획기관(ARPA)에서 창설한 연구망이다. 오늘날 인터네트의 전신이다.

DNS(Domain Name System)

사용자들이 UNIX망이나 인터네트(TCP/IP망)에서 령역이름을 리용하여 콤퓨터를 찾아 내게 하는 이름해석쏘프트웨어이다.

IMAP(Internet Messaging Access Protocol)

인터네트상에서 널리 리용될것이 기대되는 표준우편봉사기규약이다. IMAP은 사용자가 접속하여 내리적재할 때까지 들어 오는 전자우편을 잡아 두는 통보문보관고를 제공한다. IMAP4판이 가장 최신판이다.

MAPS(Mail Abuse Prevention System)

RBL(Real time Blackhole List)을 가지고 스팸을 제거하는 캘리포니아에 있는 한 비영리기관. RBL에는 스패머의 IP주소들이 있으므로 회사들과 ISP들은 들어 오는 우편을 거부하는데 그 목록을 사용할수 있다.

ORBS(Open Relay Behavior modification System)

대량전자우편통보문의 제3자(열린)중계를 허락하도록 확인된 SMTP봉사기들을 추적하기 위한 자료기지이다. ORBS는 MAPS의 경쟁대상이다.

PEM(Privacy Enhanced Mail)

인터네트상의 안전한 전자우편표준. 이것은 암호화, 수자식서명, 수자식인증서는 물론 비공개열쇠방식과 공개열쇠방식을 다 지원한다.

POP3(Post Office Protocol 3)

보통 인터네트상에서 사용되는 표준우편봉사기규약. 이것은 사용자가 접속하여 내리적재할 때까지 들어 오는 전자우편을 잡아 두는 통보문보관고를 제공한다. POP3은 선택성이 작은 단순체계이다. 모든 대기중 통보문과 부착물들은 동시에 내리적재된다. POP3는 SMTP통신규약을 사용한다.

S/MIME(Secure Multipurpose Internet Mail Extensions)

인터네트전자우편을 통하여 비본문파일을 전송하기 위한 일반방식의 하나인

데 그것은 원래 ASCII본문을 위한것이였다. S/MIME는 비밀전송에 RSA암호를 추가하는 MIME이 판본이다.

SMTP(Simple Mail Transfer Protocol)

인터네트상의 표준전자우편규약. 이것은 통보문형식과 통보문전송대행(MTA)을 정의하는 TCP/IP규약인데 전자우편을 보관하며 전송한다.

SSL(Secure Sockets Layer)

인터네트상의 주되는 보안규약. 하나의 SSL대화가 시작되면 봉사기는 자기 공개열쇠를 열람기에 보내는데 열람기는 그것을 리용하여 우연적으로 생성되는 비밀열쇠를 그 대화에 대한 비밀열쇠교환을 위하여 봉사기에 돌려 보낸다.

TLS(Transport Layer Security)

IETF에서 제정된 보안규약인데 그것은 SSL과 다른 규약을 혼합한것이다. 이것은 인터네트상의 주요보안표준으로 기대되고 있으며 SSL의 지위를 대신하고 있다. TLS는 SSL과 호환성이 있으며 Triple DES암호화를 사용한다.

UBE(Unsolicited Bulk E–mail)

요구와 허락없이 수많은 수신자들에게 보내지는 다량의 비요청전자우편. 다른 한편 스팸으로 알려 져 있다.

VPN(Virtual Private Network)

접근조종과 암호화를 통하여 개별망의 보안을 보장하는 공공망내에 구성되는 개별망으로써 대형공공망들의 기성운영설비들의 효과적리용과 그에 의한 규모확장면에서 유리한 점이 있다.

X.25 CCITT(현재 ITU)

1970년대 초에 개발되여 1976년에 발표된 처음으로 되는 국제적표준파케트교환망. X.25는 음성을 위한 공중전화체계와 류사하게 전 세계적인 범용자료망으로 설계되였으나 비호환성과 무관심성으로 하여 그렇게 되지 못하였다.

X.400

OSI와 ITU표준통신규약인데 응용프로그람계층규약(OSI모형에서 7계층). X.400은 Ethernet, X.25, TCP/IP 전화회선을 포함하는 여러가지 망전송에서 동작하도록 정의되였다.

제１４장. 쿠키와 Web Bug란 무엇인가

윌리암 티 하딩
애니타 제이 리드
로보트 엘 그레이

쿠키란 무엇이며 Web bug란 무엇인가. 이 쿠키는 식료상점에서 흔히 볼수 있는 과자의 일종인 쿠키가 아니다. 오히려 쿠키는 월드와이드Web에서 찾아 보게 되는 Web싸이트에서 만들어 져서 콤퓨터의 하드구동기에 전송되는 특이한 작은 본문파일이다. 쿠키파일들은 인터네트상에서 매번 진행되는 마우스클리크선택들을 기록한다. 어떤 URL(Uniform Resource Locator)을 건반으로 입력한 후에 열람기는 그 봉사기와 교신하여 특정Web싸이트를 화면에 연시해 줄것을 요청한다. 열람기는 그 싸이트로부터의 쿠키파일이 이미 있는가를 알아 보기 위하여 하드구동기를 검색한다. 만일 사용자가 그 싸이트를 이미전에 방문한적이 있다면 이미전에 쿠키파일에 기록된 특수한 식별코드가 확인되고 열람기는 그 쿠키파일내용을 그 싸이트에 되돌려 보낼것이다. 봉사기는 사용자가 이미전에 그 싸이트를 방문했을 때 실제로 선택했던것의 리력파일을 가지고 있다. 사용자는 이미전에 선택하였던것들이 화면상에서 강조되므로 쉽게 볼수 있다. 만일 사용자가 이 특별한 싸이트를 방문한것이 처음이라면 ID가 할당되고 이 초기쿠키파일은 하드구동기에 보관된다.

Web bug는 누가 Web페지나 전자우편을 읽고 있는가는 감시할수 있도록 설계된 Web페지 혹은 전자우편통보문상의 어떤 도형이다. Web bug는 전자우편수신자가 정보가 로출되는것을 바라든 바라지 않든 전자우편수신자의 IP(Internet Protocol)주소를 제공할수 있다. Web bug는 통보문이 얼마나 자주 전송되여 읽혀 지는가 하는것과 관련된 정보를 제공할수 있다. Web bug의 다른 용도는 아래에서 자세히 설명한다. 덧붙여 말하면 Web bug와 쿠키는 어떤 사람의 전자우편주소에 대하여 함께 사용될수 있으며 지어는 동기화될수도 있다. Web bug는 쿠키의 리용과 관련하여 조사하여야 할 긍정적, 부정적, 위법적, 비도덕적문제들이 있다. 이에 대해서도 아래에서 자세히 설명한다.

쿠키란 무엇인가

몇해전에 와서야 쿠키는 론의할만한 문제로 되였다. 그러나 이미 언급하였지만 식료상점에서 볼수 있는 Oreos나 Famous Amos라는 이름이 붙은 그런 쿠키(즉 과자)를 이야기하는것은 아니다. 이 쿠키는 Web싸이트와 콤퓨터의 하드구동기사이에서 전송되는 정보를 취급한다. 비록 쿠키가 보다 대중적인 화제로 되고 있지만 자기 하드구동기에 보관되는 쿠키를 알지 못하는 사용자들이 아직 많다. 쿠키를 잘 알고 있는 사람들은 인터네트의 사적비밀과 륜리문제를 꺼낸다. Double Click, Inc와 같은 많은 회사들은 역시 《인터네트회사들이 너무한가?》라는 질문으로 그들에 대해 소송을 제기한다.

먼저 쿠키의 기초를 명백히 할 필요가 있다. Netscape의 로우 몬탈리(Lou Montalli)는 1994년에 쿠키를 발명하였다. 그때 쿠키를 발명하게 한 유일한 동기는 직결장바구니(shopping basket)를 가능하게 하자는것이였다. 그런데 이름은 왜 《쿠키》로 달았는가. 《쿠키 … 좋은가, 나쁜가?》라는 기사에 의하면 초기에 해커들은 앤디 윌리암즈(Andy Williams)의 텔레비죤극에서 용기를 얻었다고 한다. 《쿠키곰》이라는 토막극이 자주 방영되였는데 거기에서 곰의 옷을 입은 녀석이 윌리암즈로부터 쿠키를 앗아내기 위하여 갖은 술책을 다 부린다. 윌리암즈는 항상 《쿠키가 없어. 이젠 없어. 더는 없어. … 정말 없어!》 라고 소리를 지르면서 극을 끝마치군 하였다. 해커는 《쿠키곰》이라는 이름을 달고 조종탁을 넘겨 받아 《쿠키 달라》라는 통보문을 연시하여 메인프레임콤퓨터조작자들을 성가시게 굴었다. 조작자가 건반으로 쿠키라는 단어를 입력하면 쿠키곰은 고맙다고 응답을 하고야 그만두군 하였다. 《쿠키》는 조작자의 기분만 상하게 할뿐이였다. 여기로부터 《쿠키》라는 이름이 유래되였다.

쿠키의 내용

쿠키를 처음 발견하였을 때 이 쿠키는 하드구동기의 정보를 조사해 내여 통과암호, 신용카드번호와 콤퓨터의 쏘프트웨어목록과 같은 상세한 개인정보를 수집한다는 풍설이 돌았다. 쿠키는 실행프로그람이 아니며 콤퓨터에서 직접적으로 아무것도 할수 없다는것이 밝혀 지자 이런 풍문은 없어 지게 되였다. 간단히 말하여 쿠키는 Web싸이트에 의하여 만들어 지고 콤퓨터의 하드구동기에 전송되는 작고 특수한 본문파일이다. 그것은 이름, 값, 종결날자, 개시싸이트를 포함한다. 머리부는 이 정보를 포함하며 열람기가 그것을 연시하기전에 문서로부터 삭제된다. 열람기에서 보기 또는 문서원천지령을 실행한다 하더라도 이 머리부를 볼수 없을것이다. 머리부는 쿠키가 만들어 질 때 그의 한 부분이다. 하드구동기에 운반되면 머리부는 떨어 진다. 쿠키의 나머지 부분의 정보만이 봉사기와 관련되며 그밖의것은 아무 상관도 없다.

머리부의 한가지 실례를 들면 다음과 같다.

```
Set––Cookie: NAME=VALUE; expires=DATE; Path=PATH
Domain=DOMAIN_NAME; secure
```

NAME=VALUE가 요구된다. NAME은 쿠키의 이름이다. VALUE는 사용자와는 관련이 없으며 초기에 봉사기가 선택하여 보내는 어떤 값이다. DATE는 쿠키가 얼마만한 기간 하드구동기에 존재할것인가를 결정한다. 종결날자가 없으면 쿠키는 Web열람기를 끌 때 끝난다. DOMAIN–NAME은 쿠키를 보내고 열람기가 그 봉사기로부터 파일을 요청할 때 이 쿠키의 복사본을 받을 봉사기의 주소이다. 그것은 쿠키가 유효한 도메인을 지정한다. PATH는 쿠키가 봉사기에 다시 전송될 때 보충정의하는데 사용되는 속성이다. Secure는 비밀통로가 리용되고 있을 때에만 쿠키가 전송된다는것을 지정한다.

여러가지 형태의 많은 쿠키들이 사용된다. 가장 일반적인 형태는 방문자쿠키(visitor cookie)라는것이다. 이것은 어떤 싸이트에 몇번 돌아 왔는가 하는 자리길을 보존한다. 그것은 여러번 방문되는 페지의 Web관리자에게 경고를 준다. 두번째 형태의 쿠키는 페지의 적재방법에 대한 사용자들의 선택값들을 보관하는 선택쿠키(preference cookie)이다. 이것은 홈페지주문화와 싸이트개인화의 기초이다. 페지에는 어느 색계통을 선택할것인가 또는 한번의 탐색에 몇개의 결과가 좋은가 등을 실례로 들수 있다. 장바구니쿠키(shopping basket cookie)는 직결주문에 쓰이는 대중적인 쿠키이다. 그것은 쿠키를 통하여 사용자에게 하나의 ID값을 할당한다. 사용자가 항목들을 선택할 때 이 쿠키는 봉사기의 ID파일에 있는 그 항목을 포함한다. 가장 유명하고 론할만한것은 추적쿠키(tracking cookie)이다. 이것은 장바구니쿠키를 닮았지만 항목들을 ID파일에 첨부하는 대신에 방문한 싸이트에 첨부한다. 사람들의 물건을 사는 습관은 그들로 하여금 목적하는 물건을 사는데로 마음이 쏠리게 한다. 회사들은 잠재적으로 사용자가 제공하는 전자우편을 보관하고 있다가 해당 사용자에 대하여 거두어 들인 정보에 기초하여 광고성전자우편을 보낼수 있다.

쿠키는 자료가 돌아 다니고 있을 때에만 사용된다. 사용자가 열람기에서 어떤 URL을 건반으로 입력한후 열람기는 그 봉사기와 교신하고 해당 Web싸이트를 요청한다. 열람기는 그 싸이트로부터의 쿠키파일이 이미 있는가 알기 위하여 콤퓨터를 조사한다. 쿠키파일이 발견되면 열람기는 쿠키의 모든 정보를 그 URL의 해당 싸이트에 보낸다. 봉사기가 그 정보를 받으면 해당 사용자의 물건사기나 검색행동들을 찾아 내는데 쿠키를 곧 리용할수 있다. 아무런 쿠키도 접수되지 않으면 해당 사용자에게 ID가 할당되고 다음번 방문에 리용될수 있게 쿠키파일의 형태로 그 사용자의 콤퓨터에 전송된다.

쿠키는 단순히 본문파일이며 콤퓨터체계에서 편집 또는 삭제될수 있다. Netscape Navigator 사용자들인 경우에는 쿠키를 (C:\program Files\Netscape\Users\default 또는 사용자이름\Cookie.txt)디렉터리에서 찾을수 있으며 Explorer사용자들은(C:\windows\Cookies)에서 cookies라는 폴더에 보관된 쿠키를 찾을수 있을것이다. 사용자들이 전체 쿠키폴더 또는 선택된 파일들을 삭제할 때 콤퓨터체계에는 손상이 없다. Web열람기들은 쿠키를 받아 들이기전에 사용자들에게 경고를 보내는 선택사항들을 가진다. 게다가 www.download.com에서 찾을수 있는 Zero–Knowledge systems, Junkguard 등과 같이 사용자들이 쿠키를 봉쇄하도록 하는 쏘프트웨어들이 있다.

고급한 사용자들에게 있어서 쿠키는 또한 Web리용을 개선하기 위한데 솜씨 있게 쓰일수 있다. 쿠키는 본문문자렬로 보관되며 사용자들은 쿠키의 종결날자, 령역, 경로를 편집할수 있다. 실례로 Java Script는 처리하기 편리한 문서객체의 쿠키속성을 만들어 낸다. 쿠키는 문자렬이므로 다른 문자렬정수나 변수처럼 문자렬객체의 메쏘드들과 속성들을 리용하여 조종될수 있다.

쿠키는 비록 간단한 본문파일이지만 쿠키를 설정하고 봉사기와 의뢰기사이에서 정보를 앞뒤로 문제없이 보내도록 하는데는 일련의 스크립트서술이 필요하다. 아마 가장 일반적으로 쓰이는 언어는 Perl CGI스크립트일것이다. 그러나 쿠키는 Java Script, Livewire, Active Server Pages 또는 VBScript를 사용하여서도 만들수 있다.

여기에 Java Script쿠키의 실례를 하나 든다.

```
<SCRIPT  language=JavaScript>
 function setCookie <name, value, expires, path, domain, secure> {
document.cookie = name + ” =” + escape(value) +
((expires) ?  “; expires=”+ expires : _0) +
((path) ?  “; path=” + path : _0) +
((domain) ?  “; domain=” + domain; _0) +
((secure) ?  “; secure” :_0);
}
</SCRIPT>
```

실례에서 쿠키설계는 다른 언어로 서술되였지만 처음에 고찰한 Perl CGI스크립트가 보다 일반적인데 그의 내용은 우와 같이 name–value쌍들을 포함한다. 이 개개의 스크립트들은 자기의 특수한 쿠키만을 설정하고 정정하는데 쓰이며 내용상으로는 아주 류사하다. 어느 스크립트를 사용할것인가 하는것은 작성자개인의 선택과 지식에 달려 있다.

사용자의 체계상에서 쿠키의 모양과 그 쿠키파일로부터 무엇을 알수 있는가 하는것을 실지로 판단할수 있는 가능성은 매우 제한적이며 쉽사리 안겨 오지 않는다. 사실 쿠키상의 모든 정보는 쿠키를 설정하는 봉사기에 의하여서만 정확히 알수 있다. 또한 대부분의 경우 사용자가 직접 cookies.txt파일이나 windows/cookies디렉터리로부터 본문편집기를 써서 그 파일들에 접근할 때 볼수 있는것은 해득할수 없는 수자나 콤퓨터잡음과 아주 류사한것들이다. 그러나 Winmag.com의 카렌 켄워씨(Karen Kenworthy)(고등형사프로그람작성자)는 윈도우즈콤퓨터의 모든 쿠키들을 연시하고 지적할수 있는 프로그람을 만들어냈다.

그 녀자의 쿠키보기프로그람은 일반적으로 부호화된 ID값뒤에 숨겨 지는 어떤 개인정보를 제외하고는 쿠키내의 쓸만한 모든 정보들을 다 연시할수 있다. 그림 14－1은 쿠키의 보기프로그람을 동작상태로 보여 준다.

알수 있는바와 같이 쿠키보기프로그람은 windows/cookie디렉터리내에 현재 109개의 쿠키가 있다는것을 보여 준다. 그 녀자는 사용자가 필요 없는 모든 쿠키들을 제거하기 쉽게 삭제(Delete)특징을 보기프로그람에 첨부하였다. anyuser@napster[2].txt라는 쿠키를 선택하였을 때 사용자는 그 쿠키파일은 napster.com에서 왔고 이 봉사기에만 유효하다는것을 알수 있다. 쿠키를 보낸 Web싸이트가 명백치 않다면 사용자는 그 특별한 쿠키가 실지로 필요한가를 결정하기 위하여 그 쿠키를 보낸 령역 또는 IP주소로 갈수 있다. 그렇지 않으면 그것을 삭제할수 있다. 다음에 Data Value가 02b07로 설정된것을 볼수 있는데 그것은 자기자신의 특수한 ID이다. 이 수자와 문자들은 사용자가 Napster양식에 이미전에 기입한 어떤 적절한 정보를 유지하고 있는 Napster봉사기자료기지와 호상작용한다. 다음에 창조날자(creation date), 종결날자(expiration date), 두 날자사이 평가시간을 볼수 있다. 또한 이 쿠키가 10년 지속할것이라는것을 알수 있다. 쿠키보기프로그람에는 32비트 2진수로 표시된 종결날자가 있다. 마지막으로 보안문제에 관한 작은 창이 있는데 그것은 기정값이 No로 설정된다.

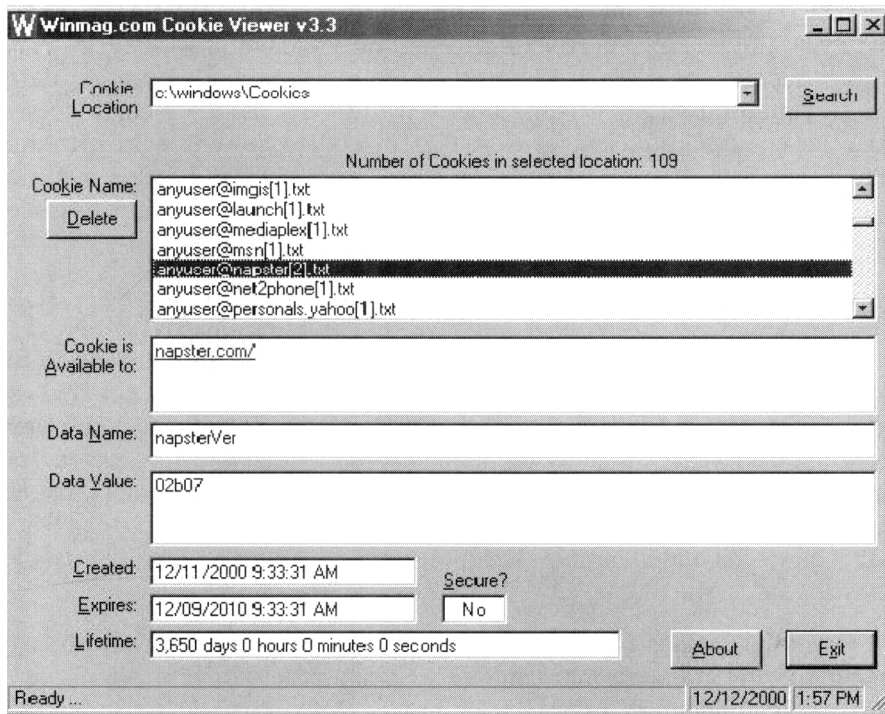



그림 14－1. 카렌의 쿠키보기프로그람

쿠키의 긍정적인 점

무엇보다먼저 쿠키의 목적은 사용자의 검색리력에 있는 자취를 보존하는데 있다. 사용자가 쿠키를 리용하는 싸이트에 접근할 때 255byte까지의 정보가 사용자의 열람기에 전송된다. 다음번에 사용자가 그 싸이트를 방문하면 쿠키는 그 봉사기로 다시 전송된다. 쿠키는 사용자가 보았거나 사용자의 보기패턴이 이전의 방문들에 기초하는 페지들의 목록을 포함할수 있다. 쿠키를 리용하여 싸이트는 사용패턴들을 추적하고 사용자들이 그 싸이트에로 접속할 때 연시되는 정보를 주문화할수 있다.

둘째로, 쿠키는 정보자원을 판매업체에 제공할수 있다. 인터네트쿠키를 리용하여 직결판매업체들은 특정고객들의 요구와 관심사로 되는 광고를 노릴수 있다. 쿠키사용에서는 소비자와 판매업체가 둘다 유리하다. 판매업체들은 보다 많은 구경군(click–through)들을 얻을수 있으며 한편 고객들은 관심이 있는 광고만 볼수 있다. 또한 쿠키는 반복되는 광고를 방지한다. Focalink와 Double Click와 같은 인터네트상업회사들은 인터네트사용자들이 같은 광고를 다시는 보지 않도록 쿠키를 실행한다. 또한 쿠키는 인터네트사용자들의 Web써핑(Web surfing)습관을 시험하여 판매업체들이 소비자들의 행동을 더잘 리해할수 있도록 한다. NCR, Inc.와 Sift, Inc.와 같은 고등자료조사회사들은 쿠키파일을 통하여 고객들에 대한 정보를 분석하고 모든 고객들의 요구를

보다 훌륭히 충족시킬수 있다.

직결주문체계는 쿠키를 리용하여 사용자가 사려고 하는것을 상기시켜 준다. 실례로 만일 어떤 고객이 한 싸이트에서 사려는 책을 찾느라고 시간을 보내는데 갑자기 련결이 끊어 졌다고 하자. 고객은 후에 그 싸이트에 다시 돌아 올수 있는데 그 항목은 여전히 자기의 장바구니에 남아 있게 된다.

싸이트개별화도 역시 쿠키의 다른 하나의 리점이다. 어떤 사람이 CNN.com싸이트에 와서 체육소식은 전혀 보지 않으려 한다고 하자. CNN.com은 그 사람에게 이것을 선택적으로 취할수 있도록 한다. 그때부터 계속(쿠키가 끝날 때까지) 그 사람은 CNN.com에서 체육소식을 보지 않게 된다.

인터네트사용자는 쿠키를 자기의 통과암호와 사용자 ID를 보관하는데 사용할수 있으며 따라서 다음번에 그 Web싸이트에 접속하려고 할 때는 그 통과암호화사용자 ID를 입력하지 않아도 된다. 그러나 쿠키의 이 기능은 콤퓨터가 다른 사용자들속에 공유되면 보안위험으로 될수 있다. Hotmail이나 Yahoo는 자기 전자우편사용자들에게 보다 빠른 접근을 제공하기 위하여 이런 형태의 쿠키를 사용하는 싸이트들이다.

쿠키는 《전자상업거래의 ＜쿠키피물＞인상박멸》에 서술된 리점을 가지고 있다. 쿠키를 리용하여 특정한 고객들이 요구하고 관심을 가지는 광고들을 묶어 줄수 있다. 이것은 수백가지의 불편하고 불필요한 광고들을 보지 않게 하는것으로 하여 사용자들에게 유리하다. 쿠키는 반복되는 배너(banner)광고를 막는다. 또한 쿠키의 리용으로 회사들은 고객들의 행동습관을 더잘 알수 있다. 이것은 판매업체들이 대부분 고객들의 요구를 만족시킬수 있게 한다. 쿠키는 그 특정콤퓨터상의 사용자의 싸이트에 보관된다. 쿠키를 불가능상태로 하기는 쉽다. Internet Explorer 4.0에서 Internet Options의 View를 선택하고 Advanced태브를 클릭하고 Disable All Cookies선택항목을 클릭하면 된다.

쿠키의 부정적인 점

쿠키기술의 리용에서 주되는 우려는 보안과 사적비밀문제이다. 일부 사람들은 쿠키가 보안위험이고 사적비밀에 침입하며 인터네트에 위험하다고 믿는다. 쿠키가 그러거나 말거나 륜리도덕은 사용자에 대하여 어떻게 정보가 수집되고 무슨 정보가 수집되며 이 정보가 어떻게 쓰이는가 하는데 기초한다. 사용자는 Web싸이트에 접속할 때마다 봉사제공자, 조작체계, 열람기형태, 모니터특성, CPU형태, IP주소, 마지막으로 접속한 봉사기와 같은 정보들을 거저 넘겨 줄것이다.

쿠키를 오용하는 좋은 실례는 사용자가 콤퓨터를 다른 사용자와 공유하는 경우이다. 실례로 인터네트카페에서 사람들은 콤퓨터의 하드구동기에 보관된 앞선 사용자의 쿠키파일을 들여다 보아서 그 사용자에 대한 기밀정보를 알아 낼수 있다.

이런 리유로부터 Web개발자는 쿠키파일을 오용하지 말며 기밀로 간주되는 정보는 쿠키파일에 보관하지 않는것이 아주 중요하다. 누구의 사회안전번호, 어머니의 처녀때 이름, 신용카드번호와 같은 정보를 쿠키에 보관하는것은 인터네트사용자들에게 위협으로

된다.

쿠키가 직결상업과 Web사용자들에게 미치는 불리한 점을 가지고 있지만 거기에는 한계가 있다. 쿠키가 무엇을 할수 있는가에 대한 여러가지 신화들이 있기때문에 다음과 같이 쿠키가 할수 없는것들을 지적해 둘 필요가 있다.

- 사용자의 하드구동기로부터 정보의 절도 또는 파손
- 하드구동기를 파괴하는 비루스설치
- 한 싸이트에서 다른 싸이트에로의 자취이동
- 허가없이 신용카드번호를 탈취하는것
- 다른 사용자의 콤퓨터에로 접근하는것
- 소비자가 자발적으로 그런 정보를 제공하지 않는 한 이름, 주소, 기타 다른 정보들을 추적하는것

2000년 1월 27일 캘리포니아주의 한 녀성은 비법적으로 소비자들의 개인정보를 얻어서 파는 Web광고상점을 고소하면서 Double Click회사에 대해 소송을 제기하였다. 그 법소송은 Double Click회사는 쿠키라는 교묘한 콤퓨터추적기술을 채용하여 인터네트사용자의 신원을 확인하고 사용자들이 Web을 돌아 볼 때 그들의 승낙없이 개인정보를 수집한다고 주장하였다. 2000년 6월 Double Click회사는 미국가족의 90%의 이름, 주소, 소매구입습관 등의 자료기지를 관리하는 직접 상업봉사회사인 Abacus Direct Corporation회사를 사들였다. Double Click회사의 새로운 사적비밀방책은 회사가 소비자들의 프로파일(사용자의 이름, 비밀번호를 비롯한 사용자고유정보–역주)을 주는 자료기지를 구축하기 위하여 쿠키에 의하여 수집된 정보를 리용하도록 계획을 세운다는것을 명백히 보여 주었다. Double Click회사는 고객들의 프로파일을 수집하면 직결광고를 부류별로 더잘 묶어 놓을수 있으며 그렇게 되면 그들의 직결활동이 더욱 활발해 지고 광고는 보다 효과성을 가지게 된다고 하면서 자기들의 프로파일수집활동의 정당성을 옹호하였다. 그리고 그것을《개별화》라고 불렀다.

전자사적비밀정보쎈터는《Double Click는 현재까지 대략 10억명의 인터네트사용자의 프로파일들을 수집하였다.》고 언급하였다. 소비자들은 이것으로 하여 Double Click가 생각지도 않게 사용자들의 개인정보에 너무 많이 접근할수 있게 한다고 생각하였다. 소비자들은 오랜기간 자기들이 비합법적인 Double Click쿠키를 받고 있다는것을 깨닫지 못하였다. 전자통신사적비밀법과 보관된 유선통신 및 거래기록접근법과 같은 련방법조항들을 위반하였다는 기록도 있다. 2000년 3월 Double Click는 사용자들이 모르게 그들의 정보를 수집한 실책에 대하여 인정하였다.

많은 사람들은 특정한 정보를 접수하든 거절하든간에 가장 좋은 사적비밀방책은 소비자들자신이《선택》할수 있게 하는것일것이라고 말한다.《Web자료의 비밀보존을 위하여》라는 기사에 의하면 텍싸스주의 플라노시에 있는 Electronic Data System(EDS)회사가 이 분야에서 가장 우수하다고 한다. EDS의 전자상업거래방책국장 빌 파울러스(Bill Poulous)는《회사들은 자기들이 개인정보를 수집하고 있다는것을 소비자들에게 이야기하여야 하며 그것으로 무엇을 하려는가를 알려 주고 자기들의 자료를 선택하거

나 그 자료의 수집을 막을수 있는 기회를 주라》고 이야기하였다. 그는 또한 그 방책들은 일반사람들이 그것을 알고 리해하고 그대로 할수 있게끔 되여야 한다고 덧붙여 설명하였다.

Web Bug란 무엇인가

Web bug는 누가 Web페지나 전자우편을 읽고 있는지 감시하기 위하여 설계된 Web페지나 전자우편상의 도형이다. 쿠키와 같이 Web bug는 싸이버공간에서 Web싸이트와 광고자들이 방문자의 행처를 추적하는것을 도와 주는 전자태그이다. 그러나 Web bug는 필수적으로 페지상에서 눈에 보이지 않을 정도로 매우 작으며 그 크기는 대략 문장끌의 종지부만 하다. Melissa비루스제작자의 추적으로 하여 잘 알려 진 www.privacyfoundation.org의 기술경영책임자 리챠드 스미스(Richard Smith)는 Web bug기술을 공개시키는 공적을 세웠다. 스미스는 다음과 같이 말하였다. 《전형적인 투명화상이고 크기는 가로 1화소, 세로 1화소인 Web페지나 전자우편통보문을 누가 읽는가를 감시하기 위하여 설계된 Web bug는 Web페지나 전자우편상의 하나의 도형이다.》 Meconomy.com의 기술경영책임자인 크라이그 나댄(Craig Nathan)은 말하기를 1×1화소Web bug는 《봉화 같다. 그래서 매번 Web페지를 때릴 때마다 하나의 핑을 전송하든가 또는 <Hi>하면서 봉사기에 응답을 보내는데 이것은 내가 누구이고 내가 어디에 있다는것이다.》고 하였다.

대부분의 콤퓨터에 쿠키가 있는데 그것은 배너광고(홈페지에 띠모양으로 만들어 붙이는 인터네트상의 광고–역주)가 연시되든가 사용자가 하나의 직결봉사에 서명할 때 하드구동기에 배치된다. 상식 있는 Web봉사기들은 배너광고를 보면 자기가 추적 당하고 있다는것을 알아 차린다. 그러나 사람들은 Web bug를 볼수 없고 반쿠키려파기들은 그것을 포착하지 못할것이다. 그래서 Web bug는 배너광고가 아직 없는 직결지역이나 추적되리라고 예상치 못하는 싸이트들에서 봉사기들을 추적하며 알아 낼수 있다.

Http://www.investorplace.com에서 Web bug에 대한 실례를 찾아 볼수 있다. 그 페지의 꼭대기에 Web bug가 위치하여 있다. Internet Explorer에서 Source메뉴의 View 또는 Netscape에서는 Page Source메뉴의 View를 선택하여 동작되고 있는 코드를 볼수 있다. 아래에서 보는바와 같이 코드는 "Investor Place"방문자에 대한 정보를 광고회사 Double Click에 제공한다.

```
<IMG SRC=”http:ad.doubleclick.net/activity;src=328142;
  type=mmti; cat=invstr;ord=<Time>?”WIDTH=1 HEIGHT=1
  BORDER=0>
```

Web페지상의 바그들에 대한 검사도 가능하다. 일단 그 페지가 적재되면 그 페지의 원천코드를 보라. 속성값들이 WIDTH=1, HEIGHT=1, BORDER=0(또는 WIDTH=”1”, HEIGHT=”1”, BORDER=”0”)인 IMG태그가 있는 페지를 찾아 보자. 이것은 작고 투

명한 화상의 존재를 의미한다. 만일 이 태그가 가리키는 화상이 현재의 봉사기가 아니라 다른 봉사기에 있다면(실례로 IMG태그가 SRC="http://"라는 본문을 포함한다면) 그것은 Web bug와 아주 류사하다.

사적비밀과 다른 Web Bug문제

Double Click나 Match Point와 같은 광고망들은 세계의 여러 지역은 물론 인터네트의 여러 지역의 특별한 Web싸이트들을 접근하는 수많은 사람들의 《독립적인 구좌만들기》를 개발하기 위하여 Web bug(《인터네트태그》라고도 함)들을 리용한다. 광고업체들은 또한 Web싸이트내에서 페지보기에 대한 통계를 낸다. 이것은 내용의 효과성을 계획하고 운영하는데도 매우 도움이 된다. 왜냐하면 그것이 목적하는 시장정보의 조사를 제공하기 때문이다(실례로 어떤 싸이트에 대한 사용자들의 많은 방문). 이와 같은 생각으로 하여 광고망들은 사용자가 방문한 싸이트의 개인프로파일을 만드는데 Web bug를 리용할수 있다. 이 정보는 자료기지봉사기에 넣어 두고 해당 사용자가 보게 되는 광고의 형태를 결정하는데 사용될수 있다. 이것은 《직접적인 광고》를 의미한다.

전자우편통보문에 리용되는 Web bug는 보다 더 해로울수 있다. Web기초전자우편에서 Web bug는 과연 그리고 언제 전자우편이 읽혀 질것인가를 결정하는데 리용될수 있다. Web bug는 수신자가 정보가 로출되는것을 바라든 바라지 않든 상관없이 수신자의 IP주소를 제공할수 있다. 기관내에서 Web bug를 보면 통보문이 몇번이나 전송되고 읽혀 질것인가 하는 착상을 줄수 있다. 이렇게 되면 직접거래에 도움이 되여 광고에서 효과가 나타난것만큼 성과를 가져다 줄수 있을것이다. Web bug는 쟝크우편(junk e–mail: 인터네트상에서 수많은 사람들에게 그들의 의사와는 관계없이 일방적으로 전달되는 대량의 광고성전자우편. 일명 spam mail이라고도 함–역주)통보문을 본 사람을 탐지하는데 리용될수 있다. 통보문을 보지 않은 사람은 앞으로의 우편목록에서 제외대상으로 된다.

쿠키의 도움으로 Web bug는 콤퓨터, 열어 본 페지, 방문시작시간 그리고 기타 세부들을 확인할수 있다. 광고봉사를 제공하는 회사들에 전송된 그 정보는 결과적으로 누군가 무엇을 사려고 또는 어떤 다른것을 읽어 보려고 같은 광고망의 다른 회사의 페지를 방문하는가를 결정하는데 리용될수 있다. 《그것은 직결보관고에서 소비자들의 활동을 수집하는 한가지 방법이다.》라고 Double Click의 기술담당책임부사장 데이비드 로젠블러트(David Rosenblatt)는 말하였다. 그러나 충실한 고객감시자인 Web bug와 다른 추적도구들은 직결콤퓨터사용자들의 사적비밀과 자립적인 활동에 위협을 증대시키고 있다.

Web bug를 Microsoft Word문서에 첨부할수도 있다. Web bug를 리용하여 문서작성자는 자기의 문서가 어디에서 몇번 읽혀 지는가를 추적할수 있다. 또한 그 감시자는 《바그가 붙은》문서가 어떻게 한사람에게서 다른 사람에게로 또는 한 기관에서 다른 기관으로 넘어 가는가를 감시할수 있다.

Word문서에서 Web bug를 리용하면 다음과 같은것을 할수 있다.

- 신용문건들의 회사로부터의 류출탐지 및 추적
- 회보 및 보고서들의 가능한 저작권위반추적
- 판권배포의 감시
- 한 Word문서에서 새로운 문서로 복사될 때 인용되는 본문의 추적

Web bug는 문서가 원격Web봉사기에 배치되는 화상파일에 련결되도록 하는 Microsoft Word의 능력에 의하여 만들어 질수 있다. 실제화상이 아니라 Web bug의 URL만이 문서에 보관될수 있으므로 Microsoft Word는 개개의 문서에 대하여 문서가 열릴 때마다 Web봉사기로부터 화상을 불러 와야 한다. 이 화상련결특성으로부터 언제 어디서 문서파일이 열리는가를 감시하도록 원격봉사기를 적당한 위치에 배치하여야 한다. 봉사기는 문서가 열리는 콤퓨터의 IP주소와 호스트이름을 알고 있다. 호스트이름은 표준적으로 기관의 회사이름으로 될것이다. 사용자의 집에 있는 콤퓨터의 호스트이름은 보통 그 사용자의 인터네트봉사제공자(ISP: Internet Service Provider)의 이름을 가진다. Microsoft Word에서는 Web화상의 련결기능을 제거하기 힘들므로 좋은 해결책이 있을상 싶지 않다. 워드문서외에 Web bug는 Excel 2000과 Power Point 2000문서에서도 사용될수 있다.

Web Bug와 쿠키의 동기화

추가적으로 Web bug와 열람기쿠키는 특별한 전자우편주소에 대하여 동기화할수 있다. 이 계책은 Web싸이트가 그 Web싸이트로 그후에 들어 오는 사람들의 신원(다른 개인정보도 포함)을 알도록 한다. 더 상세히 설명하면 쿠키가 해당 사용자의 콤퓨터에 배치되면 원래 쿠키를 가지고 있던 봉사기만이 유일하게 그것을 읽을수 있다. 리론적으로 두개의 서로 다른 싸이트들이 사용자의 콤퓨터에 제각기 특수한 쿠키를 배치하면 그것들은 각각 각자의 쿠키에 보관된 자료를 읽을수 없다. 례를 들어 말한다면 한 싸이트는 사용자가 최근에 다른 싸이트를 방문하였다는것을 알수 없다는것을 의미한다. 만일 그러나 사용자의 콤퓨터에 배치되여 있는 쿠키가 그 싸이트가 광고기관봉사기에 보낸 정보를 가지고 있고 그 기관은 두 Web싸이트들에 의하여 다 리용된다면 사태는 아주 달라 진다. 만일 이 싸이트들이 각각 자기들의 페지에 Web bug를 배치하여 광고기관의 콤퓨터로 돌아 오는 정보를 보고하면 사용자에 대한 상세한 정보는 두개의 쿠키파일들과 관련된 사용자콤퓨터에 보관된 정보를 리용하여 광고기관에로 다시 전송될것이다. 이것은 사용자의 콤퓨터가 두개의 싸이트들을 각각 방문한 콤퓨터로 확인되게 할것이다.

다음과 같은 실례가 이것을 더 정확히 설명한다. Web봉사기인 보브가 Web bug를 포함하고 있는 페지나 전자우편을 열 때 《투명한 GIF화상》이 있는 봉사기에로 정보가

전송된다. 전송되는 일반정보는 보브콤퓨터의 IP주소, 열람기형태, 연시되는 Web페지의 URL, 화상의 URL, 파일이 접근한 시간 등을 포함한다. 또한 봉사기에로 전송되면서 보브의 사적비밀정보에 대부분의 위협을 줄수 있는 정보는 그의 콤퓨터에 있는 이미 설정된 쿠키값이다.

미리 정의된 쿠키의 성질에 따라 그것은 사용자이름과 통과암호로부터 전자우편주소와 신용카드정보에 이르기까지 모든 정보를 다 포함할수 있다. 앞의 실례를 계속 들어 이야기하면 보브는 광고기관봉사기의 투명한 GIF화상을 포함하는 Web싸이트#1을 방문하자 곧 쿠키를 받을것이다. 보브는 또한 같은 광고기관의 봉사기의 투명한 GIF화상을 포함하는 Web싸이트#2에 갈 때 다른 하나의 쿠키를 받을수 있다. 그러면 두개의 Web싸이트들은 그 광고업체에 보고를 보내고 있는 쿠키들을 통하여 보브의 활동을 서로 참조할수 있을것이다. 이 활동이 계속되면 광고업체는 보브의 개별적특성을 나타내는 정보는 물론 보브와 같은 부류의 사람들의 취미와 습관 같은 정보들을 축적할수 있다.

쿠키코드가 표준화되면 각이한 봉사기들사이에서 쿠키와 Web bug가 동기화됨으로써 월드와이드Web전반에 걸쳐 정보를 공유할수 있는 기술적가능성이 주어 지게 된다. 만일 실지 그렇게 된다면 어떤 사람이 어떤 Web싸이트를 방문하였다는 사실이 많은 인터네트봉사기들을 통하여 전반적으로 퍼지게 되며 사적비밀의 침해는 끝이 없게 될것이다.

결 론

쿠키와 Web bug의 기초에 대해서는 정의, 내용, 리용성, 사적비밀우려, 동기화 등을 통하여 보여 주었다. 쿠키의 실제코드당 Web bug들에 대한 여러가지 실례들은 독자들에게 그것들을 확인하는 방법을 배워 주는데 도움이 되도록 설명되였다. 쿠키와 Web bug들을 기업활동에 리용하는 긍정적측면들이 론의되였다. 또한 쿠키와 Web bug에 관련된 사적비밀과 다른 문제들이 시험되였다. 끝으로 Web bug와 쿠키의 동기화(Word문서 포함)가 론의되였다.

그러나 우리의 론의는 쿠키와 Web bug들을 식별하고 보관하며 오늘날에 사용하는것에 기본적으로 국한되였다. 쿠키와 Web bug메타자료(자료에 대하여 보관된 자료)를 사용하면 개별적사용자의 행동에 대한 다량의 정보를 여러 콤퓨터체계환경에서 추적할수 있다. 언제인가 우리는 쿠키와 Web bug보관고에서 나오는 모든 변칙들과 소비자경향을 조사하는 쿠키 및 Web bug채취쏘프트웨어를 보게 될것이다. 그러니 우리가 지금까지 고찰한것은 빙산의 일각에 지나지 않을것이다.

참 고 문 헌

1. Bradley, Helen. "Beware of Web Bugs & Clear GIFs: Learn How These Innocuous Tools Invade Your Privacy," *PC Privacy*, 8(4), April 2000.
2. Cattapan, Tom. "Destroying E-Commerce's 'Cookie Monster' Image," *Direct Marketing*, 62(12): 20–24+, April 2000.
3. Hancock, Bill. "Web Bugs — The New Threat!," *Computers & Security*, 18(8), 646–647, 1999.
4. Harrison, Ann. "Keeping Web Data Private," *Computerworld*, 34(19): 57, May 8, 2000.
5. Junnarkar, S. "DoubleClick Accused of Unlawful Consumer Data Use," *Cnet News*, January 28, 2000.
6. Kearns, Dave. "Explorer Patch Causes Cookie Chaos," *Network World*, 17(31): 24. July 31, 2000.
7. Kokoszka, Kevin. "Web Bugs on the Web," Available: http://writings142.tripod.com/kokoszka/paper.html
8. Kyle, Jim. "Cookies ... Good or Evil?," *Developer News*. November 30, 1999.
9. Mayer-Schonberger, Viktor. "The Internet and Privacy Legislation: Cookies for a Treat?" Available: http://wvjolt.wvu.edu/wvjolt/current/issue1.
10. Olsen, Stefanie. "Nearly Undetectable Tracking Device Raises Concern," *CNET News.com*, July 12, 2000, 2:05 p.m. PT.
11. Rodger, W. "Activists Charge DoubleClick Double Cross," *USA Today*, July 6, 2000.
12. Samborn, Hope Viner. "Nibbling Away at Privacy," *ABA Journal, the Lawyer's Magazine*, 86:26–27, June 2000.
13. Sherman, Erik. "Don't Neglect Desktop When It Comes to Security," *Computerworld* 25: 36-37, September 2000.
14. Smith, Richard. "Microsoft Word Documents that 'Phone Home,'" *Privacy Foundation*. Available: http://www.privacyfoundation.org/ advisories/advWordBugs.html, August 2000.
15. Turban, Efraim, Lee, Jae, King, David, and Chung H. *Electronic Commerce: A Managerial Perspective*, Prentice-Hall, 2000.
16. Williams, Jason. "Personalization vs. Privacy: The Great Online Cookie Debate," *Editor & Publisher*, 133(9): 26–27, February 28, 2000.
17. Wright, Matt. "HTTP Cookie Library," Available: at: http://www.worldwidemart.com/scripts/.

참고Web싸이트

1. http://www.webparanoia.com/cookies.html
2. http://theblindalley.com/webbugsinfo.html
3. http://www.privacyfoundation.org/education/ webbug.html
4. http://ciac.llnl.gov/ciac/bulletins/i-034.shtml
5. http://ecommerce.ncsu.edu/csc513/ student_work/tech_cookie.html
6. http://www.rbaworld.com/security/computers/ cookies/cookies.shtml
7. http://www.howstuffworks.com/cookie2.htm

제1 5장. 가상개별망의 실현

제임스 에스 릴러

가상개별망(VPN)들은 원격접근과 소규모사무실 및 가정사무실(SOHO)지원으로부터 기업간(B2B)통신에 이르기까지의 여러가지 목적에 점점 더많이 리용되고 있다. 이 기술이 리용되기 시작하자마자 거의 모든 기업들에서 VPN들을 이런저런 형태로 리용하기 시작하였다. 기업형식이나 시장에 관계없이 VPN들은 통신과 관련된 생활의 모든 령역을 침투하고 있는것 같다. 통신을 확대해야 할 일련의 필요성으로 하여 투자의 즉시적인 효과를 볼수 있도록 VPN들을 도입할수 있다.

각이한 제품들의 리용성과 그 범위가 주어 졌으므로 VPN들의 실현은 그 어느 때보다도 쉬운것이다. 많은 경우에 VPN들의 설치와 유지는 상대적으로 쉽다. 회사들이 요구하는 많은 제품들을 보장하여야 하므로 VPN제품들은 집적도가 높다. 그렇다고 하여 VPN들이 경로조정규약, 접근조종수단 및 다른 인터네트운영기술들이 통합되여 뒤엉킨 큰 환경에서도 단순하다는것은 아니다. 그러나 VPN들은 본질상 통신가동환경의 또하나의 형식이며 또 그렇게 되여야 한다.

여러가지 제품들과 일반적으로 알려 진 VPN들의 응용프로그람뿐아니라 기술에 대한 호기심과 안전한 통신에 대한 약속으로 하여 사용할 규약선택에서 혼란만이 일어 난다. 선택할수 있는 여러가지 표준들과 류형의 VPN들이 있으며 매 표준과 류형은 자기의 속성들을 가지고 있으므로 해당 대안의 각이한 요구를 만족시킨다. 린접기술과는 달리 망의 여러가지 해결조건들을 만족시킬수 있는 속성들을 가진다. 물론 매 판매업체는 그 표준에 대하여 해석을 가하며 그것을 적용하는 방법도 동일한 토대에서 망을 구축하는 다른 사람들과는 다를수 있다. 그럼에도 불구하고 VPN들은 널리 퍼졌으며 놀라운 속도로 파급되고 있다. 앞으로 시간이 흐르고 기술이 발전함에 따라 이에 대하여 보다 더 크게 기대할수 있을것이다.

VPN들은 전통적인 광지역망들을 모방하는 통신구성방식을 제공할수 있다. 대체로 이런 응용프로그람에서는 인터네트를 리용하여 단일한 접속만 실현하여도 많은 원격싸이트 및 사용자들과 자료를 교환할수 있을것이다. 인증, 암호화 및 방책을 리용하고 최종적으로는 인터네트를 통하여 Web이라는 가상통로를 구축함으로써 여러가지 가상망들을 세울수 있다.

초기 VPN의 견지에서는 인터네트가 신뢰성이 없고 일관성이 없었다. 최근까지도 인터네트의 능력을 믿지 못하였다. 인터네트접속은 종종 성공하지 못하였고 자료전송속도는 파동이 심하였다. 많은 사람들이 대체로 인터네트를 하나의 걸치레나 하는 보안이 없는 망으로 인정하였다. 인터네트에 대한 확신이 부족한 관점에서 보면 임무가 중요하고 시간을 엄수할것을 요하는 정보통신들을 성과적으로 인터네트를 통하여 실현할수 있겠는가 하는 우려는 보안과 관련된 문제에서 더욱 심하게 나타났다. 통신속도가 너무 느려서 리용할수 없었다면 안전담보에 대하여 누가 신경을 썼겠는가. 인터네트에 대한 요구가 전반적으로 높아 지면서 그 하부구조에 대한 요구도 높아 졌다. 인터네트는 일반적으로

훨씬 더 신뢰성이 있으며 더 높은 자료전송속도가 가능해 지고 있다. 더 많은 인터네트 접근점들이 속도를 높이면 높을수록 더 좋은 신뢰성과 앞선 울타리기술이 모두 결합되여 인터네트에 기초하고 있는 광역통신용VPN들의 덕을 보도록 사람들의 마음을 돌려 세우게 되였다.

VPN의 도입을 반드시 확대해야 한다는 견지에서 이 장에서는 흔히 생각하는 방식과는 다른 방법으로 VPN을 리용할수 있는 일부 문제들을 언급한다. 여기에서 설명하는 내용은 VPN을 요란히 선전하는 사람들이 주로 제창하는 방법으로서 새로운것이 아니나 그렇다고 하여 VPN실현에서 흔히 볼수 있는 그렇게 일반적인것도 아니다. 이 장에서는 각 기관들이 자기들이 가지고 있는 환경 및 기술적조건들을 효과적으로 리용하여 어떻게 자체의 망의 기능을 훨씬 높일수 있겠는가 하는 일부 문제들을 고찰해 보려고 한다.

VPN의 기본우월성

기관들에서 VPN을 전개하는 리유가 몇가지 있다. 여기에는 자금절약과 기능제거 및 접근의 증대와 같이 단순한 목적들이 속할수 있다. 또한 엑스트라네트망접근과 그에 의하여 얻을수 있는 정보들에 대한 통제에 보다 큰 리유가 있을수 있다.

어떤 경우에도 VPN은 현존 인터네트접속을 리용하는 정보통신을 빨리 설치하게 하며 보안과 관련된 봉사의 유연성을 보장한다. 그 속성들가운데서 그 어느것도 종래의 통신에서처럼 특히 프레임중계(Frame Relay)에서처럼 그렇게 뚜렷하지 못하다. 이 두 기술을 비교하기 어려운것은 일단 가상회로들을 통과하면 그 류사성이 달라 지기때문이다. 그러나 시간과 안전성은 론의할수 있다.

프레임중계(FR)망들의 배치, 특히 제공자와 련계가 없는 새로운 FR를 배치한다는것은 그야말로 시간랑비로 될수 있다. 그 통신망을 제3자가 관리하는 경우 새로운 영구가상회로(PVC)에 주소공간을 할당하고 이 회로를 경로조정체계에 포함시키면 작업량이 너무 많아 질수 있다. 또한 모든 PVC에는 비용이 드는것이다.

보안과 관련하여 보면 통신망전송자료의 비밀성은 통신제공자에 직접 의존하게 된다. 자료를 광대역망(WAN)에 보내기전에 자료소개자가 예방대책을 세우지 않으면 그 정보에 대한 보호는 통신사업자와 다른 통신사업자와의 호상련결에서 보장하게 되여 있다.

시간은 돈이다

보는바와 같이 프레임중계와 비교하면 VPN은 빨리 설치할수 있으며 품을 얼마 들이지 않고 해체할수 있다. 실례로 인터네트접속 및 VPN설비를 가지고 있는 한 회사가 봉사를 받기 위하여 다른 기관과 림시련계를 가지고저 한다고 하자. 현재 수천개의 다른 VPN들이 여러 원격싸이트 및 사용자들과 동일하게 접속되여 가동중에 있을수 있다. 그

렇지만 물리적교체와 설비구입은 하지 않아도 되며 다만 다른 하나의 싸이트를 포함할수 있게 설정을 변경하면 된다. 최근에는 이렇게 하자면 제기된 VPN의 매 종단점의 구체적인 설정이 필요하다. 지금 많은 제품들은 VPN들의 원격관리를 할수 있는 종합적인 관리능력을 가지고 있다. 일부 제품들은 VPN에서 가동하며 다른 제품들은 SNMPv3과 같은 관리기준을 리용하여 인터네트관리를 안전하게 한다.

통신을 거의 순간적으로 절단 및 구축하는 능력이 주어 졌으므로 끊임없이 변하는 통신환경에서 VPN의 우월성은 확고하다. 일반적으로 한 기업은 정보교환을 위하여 다른 한 기업과 림시접속을 요구하게 된다. 광고회사들, 자문회사들, 정보중계자들, 병참기관들, 제조업체들은 모두 자기 고객들과 동업자들과의 통신을 요구하거나 통신을 리용할수 있다. 제한된 장소에서 그런 통신을 빨리 실현할수 있는 능력이 있다면 매우 짧은 기간내에 통신이 진행될수 있다. 일단 그러한 접속에 대한 필요가 없으면 본래의 상태로 된다. 통신계약, 투자관리 혹은 연장에 대한 어떤 우려가 없이도 VPN은 해제될수 있다.

보안도 역시 돈이다

VPN이 보장하는 보안은 명백한것 같다. 일반적으로 VPN접속은 인터네트상에서 이루어 지며 취약점들이 많은 곳을 통과하지만 자료는 인증되고 암호화되므로 보호된다. 그러나 일부 우점들은 그렇게 확고하지는 못하다. 좋은 실례는 그 기업의 여러 위치들에서 여러 외부기관들과 다중접속들을 요구하는 경우이다.

지리적으로 널리 퍼져 있는 기관은 다른 기관들과 여러 싸이트에서 여러가지 접속을 가질수 있다. 각이한 여러 곳에서 엑스트라네트와 접속되여 있는 싸이트들이 있을수 있는데 일부 경우에 매 접속은 자기의 경로기와 FR봉사제공자를 가질수 있다.

그런 환경에서는 보안에 어려운 문제들이 많이 제기된다. 한 망의 다른 망에 대한 공격들, 더욱 우심하게는 그 기관망이 제공하는 접속을 리용하는 엑스트라네트들사이의 공격을 없애기 위하여서는 접근을 엄격히 통제하여야 한다. 때때로 통신에 리용할수 있는 활동을 제한하는 경로기의 접근조종목록(ACL– Access Control List)들을 보안에 적용할수 있다. 일부 기관들에서는 방화벽뒤에 전용망을 할당하여 보안을 보장한다. 많은 경우에 보안은 중심적으로 관리하는 방화벽이면 충분하다. 유일하게 문제거리로 되는것은 많은 방화벽들이 비용이 많이 들게 되므로 제한된 요구와 수명을 가진 망들에 방화벽을 덧붙이자면 비용의 효과성이 없는것이다.

그러나 안전하고 유연한 VPN을 위하여 효과적으로 전개될수 있는 각이한 형식과 크기를 가진 비용의 효과성을 담보하는 여러가지 제품들이 있다. 경로기에서 IPsec봉사를 할수 있는 조건에서 이 제품들은 많은 경우 기초통신, 경로조정규약들, 방화벽봉사, 인증은 물론 광범위한 VPN봉사도 보장할수 있다. 결국 VPN계획은 빨리 작성되여 경로기에 실현하면 한 점을 통한 접근조종에 리용될수 있다. 경로기에 실현하는 방책은 접속할 때에 세부사항들을 리용하여 해당 통신을 식별하며 정확한 보안대책은 물론 망접근도 통제한다.

통합된 망

VPN이 산업에 처음으로 도입된것은 원격접근을 해결하기 위해서였다. 큰 모뎀묶음(modem pool)에 전화로 신청하면 류동사용자들은 흔히 무료번호나 그들이 가정사무실에 접속하군 하던 접근번호들을 제공 받았다. 원격접근해결책을 세울 때와 마찬가지로 그 비용은 시간에 좌우되였다. VPN은 원격사용자에게 인터네트접속과 가정사무실에로의 개별통로개설을 가능케 하였다. 인터네트접속은 시간제한이 심하지 않으며 일반적으로 비용의 효과성이 높았다. 한개 장치를 수천명이 동시에 리용할수 있으므로 가정사무실에서는 비용이 훨씬 더많이 절약되였다. 이 방법은 전통적인 전화가입식대안에 비하여 일대 획기적인 비약이였다.

이 기간에 많은 기관들에서는 동일한 개념을 망 대 망통신에 리용할수 있지 않겠는가고 생각하고 있었다. 이 문제는 자택근무하는 사람들에게 원격사무실 즉 가상사무실을 지원하는 형태로 시작되였다. 광대역인터네트접근을 전용으로 사용할수 있게 됨으로써 VPN리용이 폭발적으로 늘어 나 가정들과 원격사무실들에서는 비용의 효과가 크고 높은 대역너비의 접근이 가능하게 되였다.

동일한 개념들을 리용하여 전통적인 WAN을 강화할수도 있다는것이 곧 명백해 졌다. 원격사무실지원에 대한 개념을 확장하여 기관의 수많은 부분들의 싸이트들을 지원할수 있게 되였다. 통신의 요구나 대역너비가 제한된 싸이트들에는 흔히 VPN이 사용되였다. 통신에 대한 요구가 거의 필요 없는 이동업무를 기관의 일부 사람들에게 시키는것은 VPN이 고장나도 기업운영에 영향이 거의 미치지 않을것이라고 생각하기때문이다. 이런 현상이 많은것은 인터네트와 VPN기술자체에 대하여 잘 모르고 있는 사정과 관련된다.

오늘 많은 기관들은 인터네트접근점들을 여러 싸이트들에 가지고 있다. 이 점들은 다른 사무실과 동업자들사이에 VPN을 구축하는데 리용할수 있다. 전통적인 WAN기술과 VPN에 기초하여 구축한 혼합WAN의 우점들은 일정한 조건에서 명백해 진다.

론리적독립

회사들에는 흔히 하나 또는 그이상의 회사사무실이나 자료집선기들이 있다. 사무실이나 자료집선기는 다른 지사, 작은 원격사무실, 가상가정사무실, 원격사용자들에게 전자우편과 자료관리와 같은 각이한 봉사를 보장한다. 지사들과 같은 자료집선기가 없는 장소들사이의 통신은 큰 기관들의 경우에 특히 기업단위들이 여러 곳에 널려 있는 경우에 부하가 크게 걸린다.

그림 15－1은 싸이트들을 서로 련결시키는 전통적인 망을 보여 준다. FR구름은 PVC의 리용을 통하여 접속을 보장한다. 이를 위하여 원격싸이트는 FR구름에 접근해야 한다. FR봉사제공업체가 어떤 지역에 봉사를 제공하지 않는다면 그곳의 기관은 또 다른 회사를 리용하지 않으면 안되며 FR회로련결업체에 의거해야 할것이다. 이것을 피하기 위하여 일부 기관들이 VPN을 리용하게 되는것은 흔히 인터네트에 쉽게 접속할수 있는 사정과 관련된다.

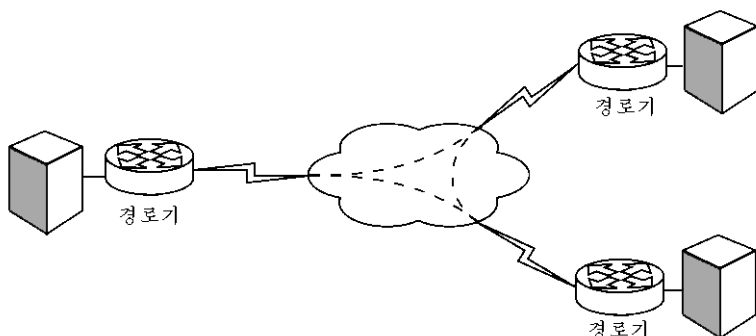



그림 15－1. 전통적인 WAN환경

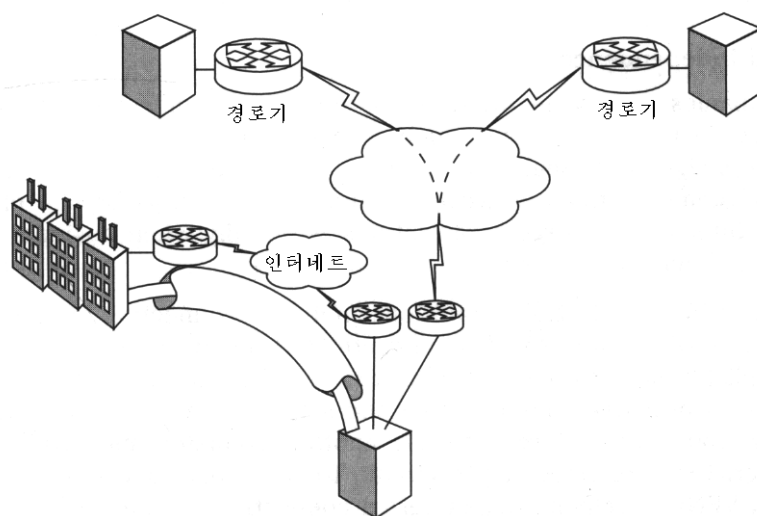



그림 15－2. 기초VPN사용

그림 15－2에서 보는바와 같이 VPN은 FR에 기초한 WAN에 신속히 병합되여 정보통신을 보장할수 있다. WAN에 1차적으로 인터네트접속을 하면 싸이트는 중앙화된 자료에 접근을 할수 있다. VPN을 리용하는 많은 원격싸이트들을 추가할수 있다. 회사싸이트에 초기투자를 한 이상 원격장소에 또하나의 싸이트를 첨부하려면 비용을 들여야만 한다. 현재 회사사무실로부터 원격사용자에게로의 접근 혹은 경영자의 집으로부터 원격사무실에로의 접근을 VPN이 보장할수 있다는것은 주목할만한것이다.

그림 15－3에서 보여 주는바와 같이 회사싸이트는 WAN을 통하여 다른 위치들에로 가는 관문으로 리용될수 있다. 이 실례에서는 VPN이 전통적인 통신망과 얼마나 류사한가 하는것을 명백하게 알수 있다. 흔히 중앙싸이트가 WAN전반에 통신을 보장하는것은 보기 드문 일이 아니다. 이 구성은 보통 《수레바퀴》(hub & spoke)라고 하며 많은 회사들은 이러한 구성구조를 리용한다.

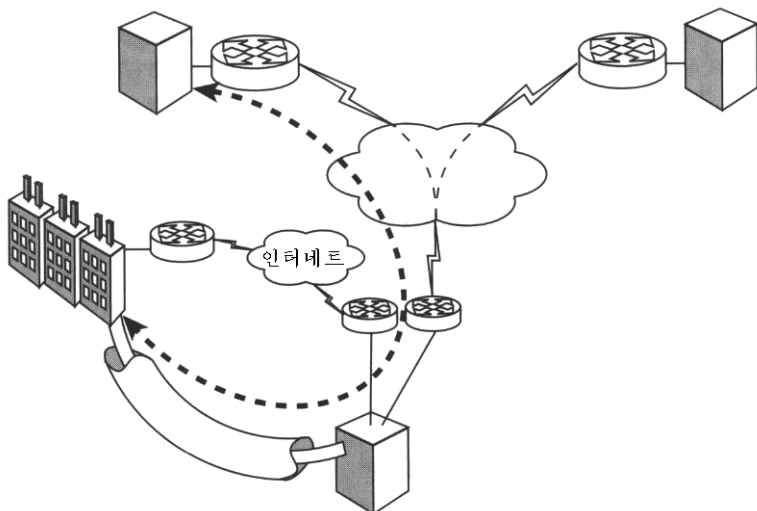



그림 15－3. VPN통합

원격싸이트들이 첨부됨에 따라 VPN은 하나의 분리된 WAN으로 리용될수 있으며 집선기싸이트는 정상적인 수레바퀴형WAN조작에서처럼 하나의 단순한 관문으로 취급된다. VPN은 충분한 유연성과 비용절약 그리고 원격접근지원을 포함하는 보충적인 우점들도 가지고 있다. 그리고 이미 리용하여 오는 WAN과 비슷하게 동작한다.

회사들이 성장하면서 매 싸이트는 WAN상에서의 인터네트전송흐름을 줄이기 위하여 인터네트접속을 보장 받는다. 인터네트접속이 많으면 많을수록 그만큼 위험성도 커진다. 그러나 자기 환경에서 인터네트에 몇개의 접속을 가지는 기관들은 FR세계에서는 불가능한 방법으로 VPN을 가동시킬수 있다.

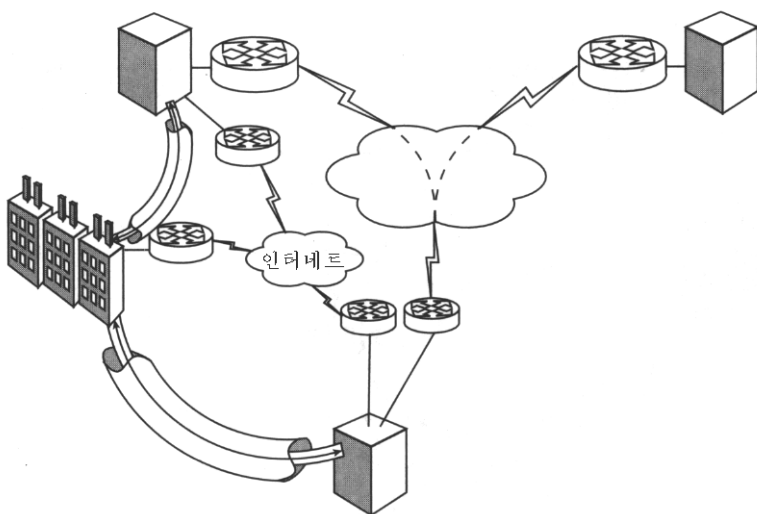



그림 15－4. 론리적자유도를 보장하는 VPN

그림 15－4에서 보는바와 같이 본래의 회사싸이트를 지나 최종목적지까지 곧바로 가닿을수 있도록 VPN을 구성할수 있다. 더욱 흥미 있는것은 그 과정이 자동적이라는것이다. 실례로 원격WAN싸이트의 주소가 10.10.10.0이고 VPN종단을 제공하는 회사싸이트의 주소가 20.20.20.0이면 원격보관고는 10.10.10.0을 요청하게 될것이다. VPN선택항목하나만이 있을 경우에 요청은 VPN을 지나서 WAN이 10.10.10.0망에로 통신을 보장하는 20.20.20.0망에로 보내지게 될것이다. 그러나 10.10.10.0망이 VPN능력들을 가지는 경우에 원격보관고는 10.10.10.0에로의 전송흐름을 그 싸이트의 VPN장치에로 보내도록 쉽게 설정될수 있다. 20.20.20.0망에서도 경우는 마찬가지다.

경로조정의 통합

경로조정규약들은 복잡한 망들에서 통신관리를 위하여 쓰인다. 이 규약들은 사용자자료와 같은 통신통로를 가지며 택한 경로를 기억한다. 실례로 거리벡토르경로조정규약은 싸이트들사이의 거리에 기초하며 련결상태경로조정규약은 련결이 이루어지도록 한다. 어느 경우에나 이런 기초원리들과 비용 및 대역너비리용과 같은 관리상 제한조항들에 기초하여 경로선택이 진행된다. 이런것들을 정의하는것은 매우 간단하다. 그러나 목적은 망자체에서 수집된 정보에 기초하여 망에서의 자료방향을 잡아주는것이다.

때문에 전통적인 망들이 VPN들을 통합함에 따라 경로결정은 새로운 의미를 띠게 된다. 실례로 세개의 싸이트를 VPN들에 옮긴 다섯개 싸이트를 가진 WAN의 경우 인터네트싸이트들사이에서는 결정해야 할 일이 거의나 없는것이다. 통신통로가 가상적이기때문에 경로조정규약은 통로를 표상적으로만 《아는것》이다. 경로조정규약파케트가 VPN에 최종적으로 유도되는 자료흐름에 주입되면 규약파케트는 파케트외피와 호상작용하는 복잡한 통신망을 통과하게 되지만 본래의 경로조정규약파케트는 자기 보호막을 쓰고 조용히 통과한다. 경로조정규약의 견지에서 보면 망은 완전무결하다.

VPN을 구성하는 큰 망들에서는 경로조정규약에 대하여 모르고 있는것은 더 말할것도 없고 또한 어떤 체계가 고장나는 경우 경로기의 인터네트쪽에서는 크게 어찌할 방도가 없게 될것이다. 원격체계가 고장나면 경로조정규약과 같은것을 리용할 방도를 찾는것이 아니라 오히려 다른 통로를 즉시 개설할수 있다. 혹은 최종목표에 대한 종속통로를 가질수 있는 또하나의 싸이트에 접속을 실현할수도 있다. 이 접속점으로는 전통적인 WAN접속점도 될수 있을것이다.

방책에 기초한 경로조정

VPN들을 기성통신망에 통합시키는 흥미 있는 변화가 일어 나고 있다. 경로조정결정들은 분할되여 각이하게 처리된다. 우선 경로조정규약은 대체로 전통적인 WAN에서는 찾아 볼수 없는 단순한 통신망들에서 쓰이며 경로조정결정들은 VPN을 보장하는 변두리장치들에로 이동하였다. 한편 인터네트우에 덮인 구름인 VPN은 모든 경로들을 다 조정하고 있는 신비스러운 《검은구멍》(black hole)으로 되고 있다.

OSPF(Open Shortest Path First)는 여러 지역개념도입에 의한 계층구조를 보장하는 경로조정규약이다. 지역들은 관리자령역들을 제공하며 최종적으로 지역 0과 작용하는 경로조정정보를 요약하는데 도움을 준다. 실례로 든 망에서 보면 지역 0에는 3개의 경로기 즉 지역경계경로기(ABR: Area Border Router외 A, B, C)들이 있다. 매 경로기는 VPN에 의하여 통신을 진행한다. 지역 0에서 정보를 공유하는외에 매 지역은 지원지역을 구성하는 원격싸이트들에 다른 경로기들을 가진다.

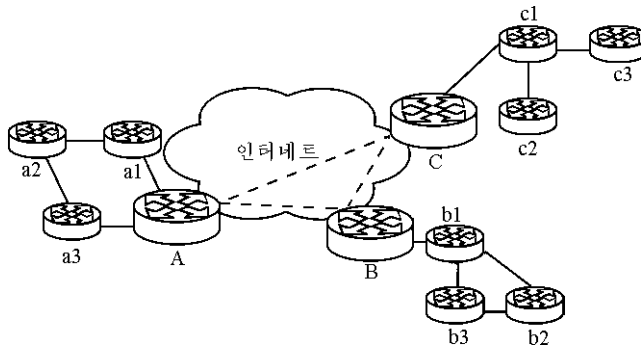



그림 15－5. VPN는 경로가 조정된 정보통신망에 영향을 준다.

그림 15－5에서 보는바와 같이 인터네트에 기초한 VPN은 지역 0이며 원격싸이트들은 3개의 부분지역들을 말한다. 망과 관련된 경로조정정보는 부분지역들과 해당한 ABR들사이에 공유한다. 그 정보는 또한 각 ABR들사이에 공유되며 최종적으로는 ABR들이 지원하는 부분지역들사이에 공유된다. 이 씨나리오에서 전체 망은 모든 통신상태들을 알게 되며 그 자료에 기초하여 결심채택을 할수 있다. 지역 0안의 련결정보를 ABR들사이에 공유하는것은 필수적이다. 그것은 부분지역경로조정자료들이 다른 ABR들과 부분지역들에 보장되게 하며 또한 가장 좋은 즉 구성된 통로가 그 통신에 리용되도록 하기 위해서이다. 실례로 전통적인 WAN에서 A로부터 B를 거쳐 C에로 통로를 설정하는것은 덜 비싸거나 더 쉬울수 있다. 이러저러한 변화를 일으키자면 통신망에서 확보된 지역 0의 특이한 정보가 ABR들사이에 공유되여야 한다.

VPN이 지역 0에 일단 도입되면 ABR들사이로 흐르는 OSPF는 교갑화된다. 때문에 지역들사이에 정보는 공유되지만 ABR들은 지역 0으로부터 정보를 거의 얻지 못한다. 실제로 얻을수 있는 정보가 거의 없는것이다. ABR들사이로 흐르는 OSPF를 통신망으로부터 얻을수 있었다면 그 통신망은 인터네트였을것이며 통로는 쉽게 변동시킬수 있었을것이다.

결과 경로규약이 원격싸이트들사이의 정보전달자로 되지만 가상정보통신에는 영향을 미치지 않게 된다. VPN이 복잡하며 인터네트로부터 정보를 거의 얻을수 없으므로(그리고 얻을수 있는것은 너무 복잡하여 사용할수 없다.) 통신방식절환을 위한 방책을 세울수도 있다. 그러나 VPN의 가상통로가 대체로 자유롭기때문에 VPN을 적용할수 있는 경우에는 그것만 구성하면 된다.

VPN이 결정된 경로조정

설명한바와 같이 상용WAN에서는 A로부터 B를 거쳐 C에로 경로설정을 하는것은 특히 A에 C를 접속하는것이 실패하는 경우에 적용할수도 있는것이다. 경로조정규약에서는 고장이 있는 경우에 B를 거쳐 경로조정을 다시 하는것이 실행할수 있는 대안으로 될수 있다고 한다. VPN에서는 이것이 구성에 따라 다를수도 있지만 더욱 심해 질수 있다. 실례로 인터네트접속이 싸이트 C에서 끊어 졌다고 하자. 그런데 c1로부터 b2에로의 접속과 같이 싸이트 B에는 자기의 하위지역싸이트들이 있게 된다. ABR들에는 다른 경로도 있지만 너무 비싸므로 사용할수 없다. 인터네트접속이 끊어 지는 경우에 VPN은 실패하며 경로조정규약은 통과할 VPN이 없기때문에 결심채택을 할수 없다. 한마디로 말하여 그 자료와 경로조정규약의 출구점은 오직 인터네트대면부이다. 이 점에서 VPN방책은 수신지에 기초한 특정된 VPN을 통한 정보를 접수하고 경로를 설정한다.

이 문제점을 해결하기 위하여 VPN체계들은 경로조정규약에서 배울수 있으며 학습하는것을 자기 방책에 포함시킬수 있다. 경로조정규약이 대면부에 주입되고 그것이 통과하는 최종 VPN이 방책에 의하여 결정되기때문에 그 방책은 A와 B사이에 VPN이 사용될수 있다고 결론을 내릴수 있는것이다. 그것은 c1과 b2사이에 있는 A와 C지역들사이에 다른 통로가 있는 사정과 관련된다.

VPN은 그것의 VPN들을 경로조정규약에로의 통로들로 광고할 필요는 없다. 그것은 통로들이 인차 만들어 졌다가 없어 질수 있기때문이다. 경로들을 창조하고 삭제하는것은 경로조정규약을 크게 파괴할수 있다. OSPF와 같은 많은 경로조정규약들은 새로운 경로가 발견되거나 이미 있던 경로가 삭제되자마자 합쳐 지는것은 아니지만 경로가 나타나거나 사라지는 빈도수와 지속시간에 따라 영향을 받는다.

방책안과 경로조정규약의 복잡한 결합에서의 최종장애는 한 위치에 있는 인터네트에 대한 접속이 여러개 있을 때 나타난다. 이 시점에 경로조정에 대한 두 갈래방법은 제3의 방법을 요구한다. 전형적으로 경계관문규약(BGP)은 하나의 기관에 대한 다중접속을 관리하기 위하여 ISP들이 리용하는 규약이다. 그 기관은 ISP의 BGP경로조정표를 통하여 ISP로부터 인터네트에로의 경로들을 알게 되며 또한 ISP는 고객의 구내설비에서의 변화들을 알게 된다. VPN체계들에서는 다중경로들을 고려해야 한다. 그러나 싸이트들사이의(IP주소변화와 같은) 론리련결이 파괴되지 않는 한 VPN은 경로가 변경되여도 작용할것이다.

VPN은 전형적으로 접수지에 따라 경로를 설정하며 종단점은 방책에 의하여 식별되며 해당 VPN종단점에 자료를 보내게 된다. VPN장치가 경로조정규약을 학습하기때문에 이 장치들은 경로조정규약대용품으로 될수 있으며 경로조정정보의 공유를 서로 보이지 않게 완전무결하게 진행할수 있다.

WAN의 부하경감

VPN들의 가장 명백한 사용법의 하나는 WAN부하를 경감하는것이다. 그 전제는 WAN을 교체하는것이 아니라 강화하는것으로서 VPN하부구조를 리용하는것이다. 보충투자나 복잡한 조종이 없이도 VPN들을 실행할수 있으며 WAN과 협력하면 보다 큰 흥미있는 결과를 얻을수 있다.

VPN이 WAN의 대용으로 실현될 때에는 새로운 하부구조의 가상적성격이 스스로 쉽게 실현되게 된다. 원래 원격접근을 위하여 준비된 현존하부구조를 가지고 그것을 원격사무실지원구조에 맞추어 동작시켜 WAN부하경감을 보장하라. 이 개념들의 대부분은 준비계획이 포괄적인 경우에 초기투자에서부터 실현을 볼수 있다.

시간에 덜 민감한 통신망들

오늘의 기술적환경에서는 모든것이 다 민감한듯하다. 그러나 시간에 민감하지 않는 많은 콤퓨터사용자들이 사용하는 응용프로그람들도 있다.

전자우편은 채트와 같은 다른 응용프로그람에 비하여 시간에 민감하지 않은 응용프로그람의 한가지이다. 더욱 흥미 있는것은 많은 회사들에서 전자우편이 기업운영의 중요한 한몫으로 되는데 이 전자우편의 즉시배달은 예견되지도 요구되지도 않는다. 전보를 몇분 기다리는것은 거의 문제로 되지 않는다. 일부 경우에 전자우편은 기관들의 생명선으로 되는것외에 자료공유가동환경으로 리용된다.

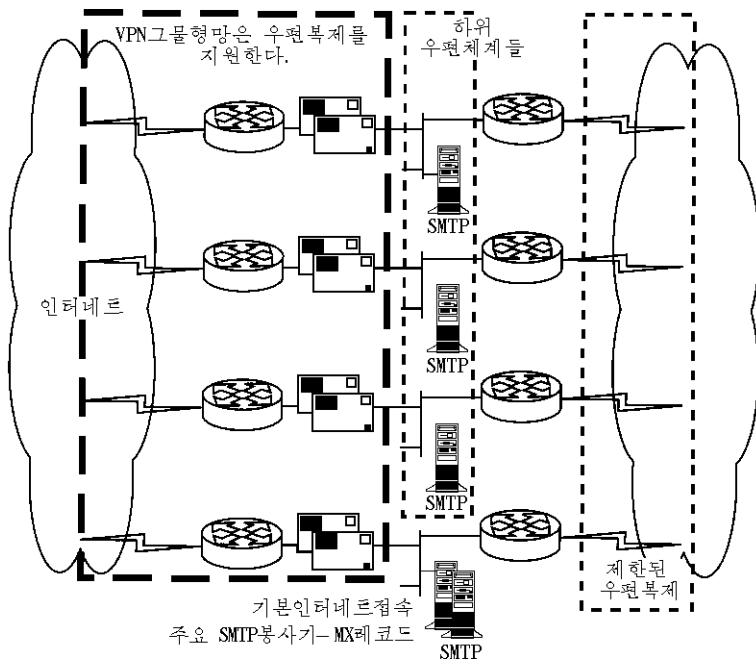



그림 15－6. VPN은 대용통신 또는 특정응용을 보장한다.

전자우편은 통신망에 큰 부담을 줄수 있다. 늘어 나는 전자우편의 요구에 맞게 오직 능력을 높이기 위하여 일부 통신망들이 솜씨 있게 가동된다고 하는것은 말이 되지 않는다.

VPN망은 WAN과 꼭같이 구성되여 특수응용에 리용될수 있다. 실례로 그림 15－6에서처럼 VPN은 한 령역전반에서 전자우편중계를 위한 통신가동환경으로 될수 있다.

많은 전자우편하부구조들에서 우편봉사들사이에 협력하는것은 최종수신지에 전자우편을 보내기 위해서이다. 공공우편봉사는 회사본부의 한 점에서 인터네트에 접속된다. 전자우편이 원격싸이트에 있는 사용자에게 접수되는 경우 1차적인 봉사기가 사용자의 우편통을 가지고 있는 봉사에 그 전자우편을 보내면 그 전자우편은 후에 본문에서 전달된다. 우편봉사기들은 론리적으로 접속된다. 또한 싸이트와 같이 봉사기들을 관리단위로 묶어주는 호상관계가 수립된다.

봉사기들사이의 련계는 정상통신통로로부터 VPN방향으로 자료흐름을 보내는 식으로 구성된다. 우점은 인차 명백해 져야 한다. 큰 배달품목록들, 소식지들, 일반통신물들을 인터네트로 내보내면 거기에서는 대역너비제한이 있어 속도가 느리지만 대신 WAN은 그 부담에서 벗어 나게 된다.

WAN을 통과하는 다른 자료흐름에 관계되는 전자우편의 량에 따라 실제적인 비용절약은 초기 VPN의 실행기간에 생긴 본래의 절약이상으로 실현된다. 실례로 WAN에서 대역너비요구가 줄어 든다면 비용도 또한 줄어 든다.

VPN의 리용은 값 비싼 WAN고리들을 통하여 응용프로그람을 얼마 쓰지 않는 국제회사들에서 특별히 의의 있는것이다. 어떤 큰 기관들은 우편물송달공정을 리용하여 부하를 줄이고 다량처리하여 세계적으로 노력을 합친다. 이 우편물묶음은 VPN으로 쉽게 배달되여 시간에 더욱 민감한 응용프로그람비용의 효과성이 높지 못한 WAN의 부하를 줄이고 있다.

우편물송달의 또하나의 실례로서는 소매업에서 보게 된다. 많은 회사들이 운영을 묘하게 하여 판매점(POS)정보를 수집하고 신용장검증, 현지상품시장과 같은 제한된 현지공간들을 보장한다. 모든 공간들이 전국적 또는 전 세계적규모에서 기업을 관리할수 있게 정보를 가정사무실에 보낼 필요가 제기될 때가 다가온다. 위성으로 상점들(전국적으로 거의 120개 상점들)에 통신을 보장한 일이 있다. 매 위치에 경로기가 있어서 POS체계, 전자우편 그리고 어떤 경우에는 전화선들에 IP접속성을 보장하였다. VSAT봉사비와 지상국장비가 협력함으로써 인터네트접속과 VPN은 거의 40%의 비용을 절약하였으며 대역너비는 50%나 늘어 났다. 결과 우편송달시간은 짧아 졌고 최종적으로 위험한 상태에 있었던 처리주프레임주파수가 늘어 나게 되였다.

한 문제를 해결함으로써 여러가지 문제가 풀렸을뿐아니라(대역너비를 늘이고 가공주파수를 늘이게 된것) 매 상점들은 VPN능력을 가지게 되였다. POS응용능력이 커짐에 따라 지역제품공급을 직접 할수 있도록 상점사이의 결제가 가능하게 되였다. 즉 등록기스캐너(register scanner)는 회사사무실에 의뢰하지 않고 고객이 요구하는 제품이 있는 위치에서 제일 가까운 곳에 상점을 정할수 있다. 이것이 혁신이 아니라 그런 거래를 위하여 활력 있는 VPN을 창조하는것이 혁신이다.

보안은 최종적인 우월한 부하경감이다. 물론 보안은 VPN들을 위한 큰 판매점이며 이 말들은 때로는 서로 동떨어 져 있는듯 하다. 그러나 이 장에서는 암시된 보안보다 오

히려 통신기술의 리용에 대하여 언급한다. 보안은 실제적인 재부이다. 실례로 전송시 전자우편을 보호하도록 전자우편부하경감도해를 구성할수 있다. 조작체계수준에서 매 우편봉사들사이에 VPN을 창조함으로써 분야안에 있는 모든 교환의 암호화를 실현할수 있다. 우편암호화프로그람을 널리 리용할수 있음에도 불구하고 많은 사용자들은 그것들을 사용하지 않는다. 기관에서 사용자들에게 최종적으로 전송내용을 암호화하도록 할 때에는 행정관리열쇠를 넣어 주어 불만스러워 하는 종업원이 자료를 빼내지 못하게 해야 한다.

VPN의 보안에는 우점이 있다. 해당 부문안에서 자료흐름이 암호화되면 사용자들은 더는 어쩔수 없게 된다. 물론 이것을 직접 PGP(Pretty Good Privacy)또는 증명서와 비교할수는 없다. 그러나 그것은 일반관측자가 흘러 가는 전자우편에 접근하지 못하도록 하는 것이다. 부문안에서 배달을 위한 암호화를 적용하지 않는 모든 전자우편체계에서 전자우편은 모든 점에서 로출된다. 즉 인터네트와 인트라네트에서 그러하다.

장애넘기

VPN에서 흥미 있는 측면의 하나는 VPN이 구성되면 선택의 세계가 시작되는것이다. 하나의 점(그것은 또한 단일원가로 인정될수 있다.)을 통하여 여러가지 가상접속들을 다중화함으로써 본래의 투자를 리용하여 여러가지 다른 기회들을 택할수 있게 된다.

한가지 실례는 WAN장애넘기이다. WAN장애넘기는 VPN과 WAN의 합침과 같은것이다. 그러나 WAN하부구조의 어떤 곳에서 고장으로 하여 막히군 하는 원래의 통화량의 일부나 전체에 VPN이 후보경로를 보장할수 있다.

시장의 실례를 보자. 전국의 각이한 의뢰기에게 응용봉사뿐아니라 FR봉사를 제공해주는 Phoenix라고 부르는 한 봉사제공자(SP)는 고객 및 봉사련합기업체들을 많이 가지고 있다. 일부 의뢰기들은 간단한 FR봉사를 요구하며 다른 고객들은 인터네트접근을 위하여 SP를 리용한다. 이 의뢰기들중 많은 고객들은 ERP체계, 인적자원체계, 전자우편, 정보안내체계, 싸이트외부보관 그리고 협력도구들의 말단사용자들이다. 봉사수준을 유지하기 위하여 Phonenix는 통신망관리와 의뢰기들, 응용프로그람들과 정보통신들에 대한 지원을 보장하는 망운영쎈터(NOC)를 유지한다.

FR가 고장이 나는 경우에는 FR고객들을 위하여 VPN을 동작시켜 응용프로그람을 지원할수 있다. 많은 기관들은 인터네트는 물론 전용통신망도 가지고 사활적인 통신을 보장하고 있다. 접속에 의거하여 다른 망을 효과적으로 리용하면 큰 장애를 극복할수 있는 기회들을 마련할수 있다.

그림 15－7에서 볼수 있는바와 같이 전용접속은 인터네트접속과의 협력에 의하여 창조될수 있다.

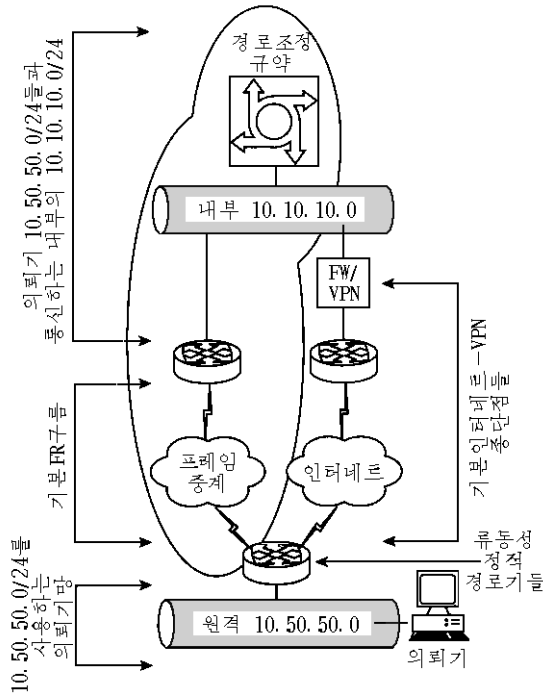
Phoenix에는 표준FR구름이 있어 의뢰기들을 지원한다. 이 통신망은 기본교환기를 통하여 NOC에 접속된다. VPN공급장치는 교환기에 접속된다. 이 실례에서는 방화벽이 VPN접속장치이기도 한데 이 방화벽이 인터네트에 련결되여 있다. 의뢰기망에는 두개의 대면부가 설치된 경로기가 있다. 하나는 전용회로접속을 위한것이고 다른 하나는 인터네트를 위한것이다.

주의: 의뢰기망상에 하나의 경로기가 있으면 Phoenix는 물론 인터네트와의 통신은 가능하게 된다. 그림에는 간단히 표시되여 있지만 가능하면 여러개의 경로기들이 기능상 영향이 없이 구성에 리용될수 있다.

그림 15－7. 후보적인 통신 혹은 특수응용을 제공하는 VPN

경로조정규약과 VPN에 대하여 앞에서 실행한대로 보면 VPN상에서는 경로조정규약을 적용할수 없는것이다. 사실 두가지 중요한 원인으로 하여 이 경우에 그런 적용을 할수 없다. 경로조정규약은 다중방송식이나 많은 방화벽들은 다중방송에 적합하지 않다. 또한 경로조정규약들이 방화벽을 지나도록 하는것은 그것이 비록 VPN을 위한것이라고 하더라도 아주 안전하지는 못하다.

경로조정규약제한들을 수용하자면 두가지 안을 택하게 된다. 첫째안은 많은 고객들과 그들의 망을 유지하는 FR구름을 통하여 표준적인것으로 리용되는 경로조정규약이다. 둘째안은 고객의 경로기에서 류동하는 정적경로들을 리용하는것이다. 한마디로 말하여 자동경로령역이 삭제될 때 류동하는 정적경로는 경로조정표로 옮겨 진다. 실례로 OSPF가 경로를 학습하면 경로는 경로조정표의 웃부분으로 옮겨 질것이다. 경로가 무효로 되여 경로조정표로부터 그 경로를 삭제하면 정적경로는 앞서게 된다.

OSPF가 FR를 Phoenix에로 되돌아 가는(행정관리비용에 의하여) 기본통신으로 보는 조건에서 해결안은 정상적으로 적용된다. 회로가 장애를 받는 경우에는 FR구름에로 통화흐름을 보내는 의뢰기의 경로조정표에 있는 경로를 OSPF가 삭제하게 되며 인터네트경로가 대신 들어 가게 된다. SP에 필요한 파케트가 대면부에 주입될 때 VPN방책은 통화흐

름을 식별하게 되며 봉사제공자가 있는 VPN을 창조하게 된다. VPN이 창조되기만 하면 VPN을 통하여 SP망에 자료가 자유롭게 흘러 간다. 자료가 의뢰기에 되돌아 올 때에는 그쪽의 FR경로기가 동일한 경로를 선택하여 그 파케트를 VPN장치에로 보내기때문에 그 자료는 VPN장치에로 갈수 있는것이다.

VPN에서의 장애극복은 VPN이 얼마나 빨리 구축되는가에 따라 일정한 시간이 걸린다. 그와는 대조되게 장애대체는 즉시적이다. FR회로가 다시 직결될 때 OSPF는 련결을 탐색한다. 그리고 일단 그 련결이 정상이라면 경로조정규약은 새로운 경로를 경로표에 다시 놓는다. 바로 이 순간부터 통화흐름은 FR구름을 통하여 움직이기 시작한다. 흥미 있는것은 FR회로가 VPN의 수명이 끝나기전에 장애를 받게 되면 장애극복도 거의 순간적인것으로 된다는것이다. VPN이 휴식상태에 있으므로 첫 파케트는 즉시 송신된다.

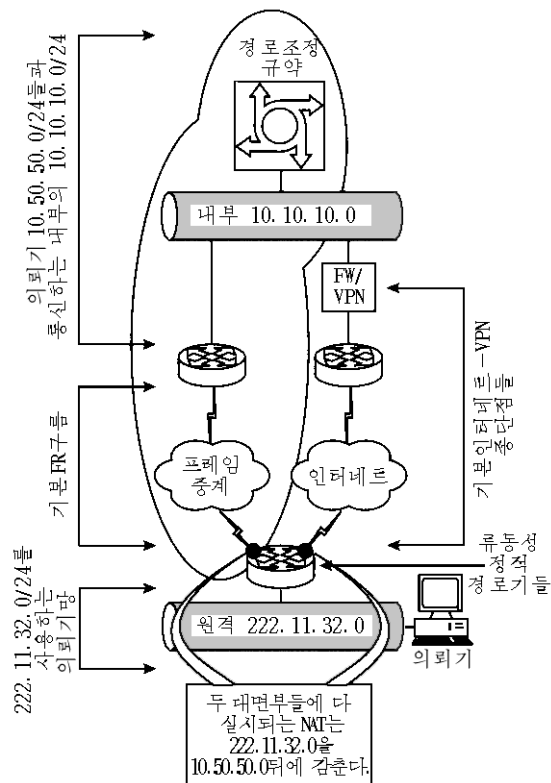



그림 15—8. 망주소변환을 사용하는 VPN장애극복

이 안과 관련하여 두가지 문제가 주목된다. FR구름이 완전히 장애를 받는다면 VPN을 예비로 가지고 있는 FR고객들은 동시에 VPN을 요구하게 되여 분명히 VPN체계는 과중한 부하를 받게 될것이다. 그런 문제를 해결하는데는 두가지 방안이 있다. 부하관리해결책은 통화흐름을 VPN장치들에 다시 보내여 모든 체계들에 그 부하를 분

산시키는것이다. 값 눅은 방법은 VPN의 의뢰기경로조종방책을 수정하여 VPN의 다음 장치가 아니라 다른 장치에로 가도록 하는것이다. 한마디로 말하여 부하를 수동적으로 분산시키는것이다.

다른 문제들이 제기되는 경우는 인터네트의 경로화가 가능한 IP주소들 혹은 다른 방안을 쓰는 망에 FR접속을 SP가 요구할 때이다. 이런것은 흔히 문제가 아니지만 SP가 관리하여 봉사를 보장해야 하는 고객구내설비(CPE)가 있다. 그 실례로는 응용관문봉사기를 들수 있다. NOC는 IP주소한조를 가지고 FR상의 장치들을 관리하게 된다. 그러나 장애극복후에는 그 IR주소들이 변할수도 있다.

그림 15－7과 류사하게 그림 15－8에서는 NAT(망주소변환)를 리용하여 의뢰기에서 관리요소들의 원천IP주소에는 관계없이 SP의 NOC가 언제나 같은 IP주소를 감시하도록 한다.

결　론

VPN이 기술계에 소개되였을 때 1차적인 구조는 망 대 망 VPN이였다. 일부 판매업자들은 VPN기술의 류동사용자측면을 강조하였다. 원격사용자지원은 VPN기술의 특징으로 되였다. 이것은 판매자가 강조하는 문제때문이였다. 그리하여 인터네트는 안전한 수단으로 인정되지 못하였다.

오늘 원격접근 VPN은 표준으로 되고 있으며 5,000단위의 접속을 동시에 지원하는 능력은 일반제품에서 흔히 보게 된다. 그러나 기성의 망하부구조들을 대신하는 VPN정보통신은 언제나 큰 호평만을 받은것은 아니다.

VPN들은 《안전원격접근》해결책으로 인정되였고 따라서 공공망을 통한 가상접속의 가치는 앞으로 충분히 탐구해야 할 문제로 된다. 최종설계에서 기본개념들이 리해되고 접수되고 발전되는 한 가능한 모든 기능들을 리용하는것은 분명 능력에 달려 있다고 보아야 할것이다.

제16장. 무선국부망보안

맨디 안드레스

무선국부망들은 이동성을 보장한다 . 회의장에 무릎형콤퓨터를 휴대하고 들어 가고 싶어 하지 않는 사람이 어데 있겠으며 또 망케블에 대한 걱정도 없이 완전한 망접근을 가지고 싶어 하지 않을 사람이 어데 있겠는가. 제작회사들은 지어 무선LAN(WLAN)을 리용하여 지금까지 망에 케블을 쓰는 방법으로는 접근할수 없는 작업현장의 기계들을 감시하고 있다. 이동성과 접근성이 높아 져 통신은 개선되고 생산능률과 효과성이 높아 졌다.

무선LAN은 또한 비용에서도 혜택을 주게 된다. 9유선통신을 설치하고 구성하는데는 비용이 많이 든다. 특히 산간오지 같은 곳에서는 더욱 그렇다. 모든 구성요소들을 제대로 설치하고 련결시키자면 흔히 사다리, 보조천정, 무거운 가구, 무릎받치개들과 많은 시간이 필요하게 된다. 그러나 이와는 반대로 무선LAN을 설치하기는 쉬운것이다. 접근점을 접속하고 무선NIC를 설치하면 망설치는 다 끝난다. 접근점은 무선장치들에 대하여 관문작용을 하는 장치이다. 이 관문을 통하여 무선장치들은 망에 접근한다(그림 16−1을 보라).

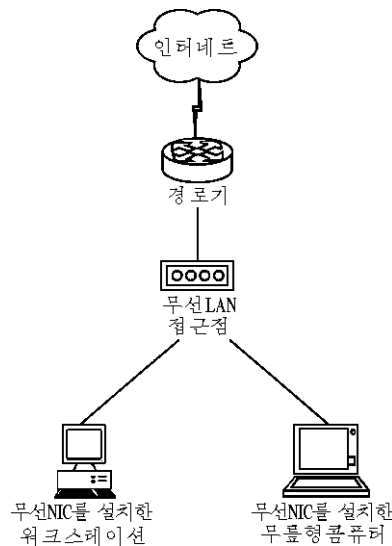



그림 16−1. 망관문으로 쓰이는 무선접근점봉사기

기동성과 비용의 효과성이 높아짐에 따라 무선LAN들은 대중화되고 있다. Gartner Group의 추산에 의하면 무선LAN수입액은 2001년에 총 4억 8천 7백만딸라에 달하며 설치된 무선LAN의 총액은 2004년이면 358억딸라로 증가될것이라고 한다. 무선LAN시장은 다음 몇해동안 해마다 25%씩 늘어 나게 되여 2000년에는 7억 7천 백만딸라였는데 2004년에 22억딸라로 늘어 날것이라고 Cahner In–Stat Group은 예언하였다. 우의 두 예측은 크게 차이나지만 한가지 공통점을 시사한다. 즉 많은 새 무선LAN이 전개될것이며 지금 설치되여 있는

것들은 확장될것이라는것이다. 이렇게 증가될수 있다고 보는것은 속도가 증가하고 가격이 인하되였으며 업계의 광범한 지원속에 공식표준이 지난 해에 채택되였기때문이다.

표 준

무선LAN에 대한 보안문제를 론의하기전에 통신의 기초로 되는 표준에 대한 론의가 중요하다. 1997년 6월 IEEE(전기 및 전자공학자협회)는 무선LAN들의 초기표준을 IEEE802.11로 결정하였다. 이 표준은 1과 2Mbps의 자료속도를 가진 2.4GHz동작주파수를 규정하며 주파수도약 및 직접렬을 리용하여 확산스펙트르변조의 두 비호환성형식들가운데서 하나를 선택하는 능력을 규정한다. 1999년 후반기에 IEEE는 초기 802.11표준에 두 보충표준 즉 802.11a와 802.11b를 발표하였다.

802.11b는 초기표준처럼 2.4GHz대역에서 동작한다. 그러나 자료속도는 1Mbps만큼 높을수 있으며 오직 직접렬변조만이 결정된다. 802.11a표준은 5.4Mbps까지의 자료속도를 가진 OFDM(직교주파수분할다중화)를 리용하여 5–9Hz대역에서 동작을 결정한다. 이 표준의 우점들은 능력이 보다 높고 다른 형태의 장치들에 대한 RF간섭이 적은것이다. 802.11a표준은 있지만 현재 시장에는 제품들이 없다. 그런 제품들은 2001년 4/4분기부터 구입할수 있게 된다. 802.11a와 802.11b표준들은 다른 주파수들에서 작용한다. 그리하여 그것들이 호상작용할수 있는 기회는 거의 없는것이다. 그러나 신호중첩이 없으므로 그것들은 한 망에서 공존할수 있다. 일부 판매자들은 앞으로 802.11a와 802.11b를 갖춘 2중무선체계를 제공하게 될것이라고 한다.

유럽은 유럽원격통신표준연구소(ETSI)의 주관하에 HiperLAN/2표준을 개발하여 문제를 복잡하게 만들었다. HiperLAN/2와 802.11a는 일부 류사성을 가진다. 두 표준은 OFDM기술을 리용하여 5GHz범위에서 자기 속도를 얻게 된다. 그러나 그것들에는 운용호환성이 없다.

이 장의 마지막부분에 가서 802.11b무선 LAN에 대하여 집중적으로 토론하게 되는데 그것들이 현재 설치된 기지를 포함하고 있기때문이다.

보 안 문 제

무선LAN은 중요한 보안문제들을 안고 있다. 기정구성, 망구성방식, 암호화약점 및 물리적보안은 다 무선LAN설치를 위한 문제들을 초래하는 지역들이다.

기 정 설 치

이미 설치된 대부분의 무선망들은 임의의 무선NIC가 어떤 형태의 인증도 없이 그 망에 접근할수 있도록 한다. 누구나 휴대형콤퓨터를 손에 들고 쉽게 다니면서 많은 망접

속을 할수 있다. 무선LAN관리자들은 라지오파가 케블보다 은밀히 도청하기가 더 쉽다는 것을 리해할수도 있다. 그러나 그들은 라지오파가 정말 얼마나 취약한가 하는것을 리해하지 못할수도 있다.

무선ISP들은 그 무선망구성들에 대하여 잘 알아야 한다. 누군가 인증도 없이 그들의 망에 접근할수 있다면 그것은 본질상 봉사를 훔치고 있는것이다. 무선ISP는 소득을 얻지 못하고 있으며 비법적인 사용자는 가치 있는 대역너비를 잡고 있는것이다.

사용자가 비법적이든 합법적이든 관계없이 무선망에 접근하는 경우 봉사기나 응용프로그람에 접근하지 못하게 하는 유일한 방도는 내적인 보안통제이다. 이런 통제가 약하거나 없으면 비법사용자가 무선LAN을 통하여 어떤 망에 쉽게 접근하고 다음에는 내적인 약점을 깡그리 리용하여 그 망을 완전히 장악할수 있다.

봉사거절공격은 또한 무선망에 대한 아주 실제적인 위협으로 된다. 무선망에서 임무가 매우 중요한 체계가 운영되는 경우 파괴나 기관에 재정적손실을 줄 목적이 있다면 그 체계에 접근할 필요가 없다. 공격자들은 위조무선전송을 망에 범람시키기만 하면 된다.

위 험 완 화

기업과 생산환경에 무선LAN들을 리용하기 위해서는 오늘의 제품과 표준에서 본래의 위험을 줄여야 한다. 기업수준의 무선LAN보안에서는 두가지 기본 문제가 제기된다. 다시 말하여 합법적사용자만이 망에 접근해야 하며 무선통화를 도청할수 없게 해야 한다. 802.11b표준에는 일부 보안장치들이 포함되여 있지만 그 규모조절성은 확실치 않다.

매체접근조종(MAC)주소

무선망에 대한 접근을 안전하게 하는 한가지 방법은 알려 진 주소들에서 출발하는 파케트들만 접근점들이 통과시키도록 지령을 주는것이다. 물론 공격자들이 MAC(매체접근조종: Media Access Control)주소들을 위장할수도 있다. 그러나 공격자는 합법적사용자의 이써네트카드의 주소를 알아야 성공할수 있다. 그런데 많은 무선카드들은 그 표면에 MAC주소들이 찍혀 있는것이다.

사용자와 관리자가 카드주소를 안전하게 할수 있다 하더라도 또한 그들은 매 접근점에 대한 유효한 MAC주소목록을 작성하고 유지하며 분배하여야 한다. 이런 보안방법은 비행장, 호텔 및 회의장에서 쓰이는 많은 대중WLAN응용에서는 가능성이 없다. 그것은 그 응용들이 그 사용자공동체를 사전에 알지 못하기때문이다. 또한 접근점은 허락되는 주소번호에서 일련의 제한이 있다.

봉사모임식별자

접근제한에 리용될수 있는 접근점에 대하여 설정해야 하는 다른 하나의 문제는 SSID(봉사모임식별자)로 알려 진 망이름이다. 한 접근점을 구성하여 의뢰기가 그에 접속하게 하거나 의뢰기가 특별히 그 접근점을 이름으로 요구하게 할수 있다. 이것이 주로 보안특성을 의미하지는 않지만 접근점을 설정하여 SSID를 요구하는것은 ID로 하여금 그룹공동통과암호로 될수 있게 한다.

그러나 통과암호방식에서처럼 더 많은 사람들이 통과암호를 알면 알수록 비법사용자가 람용할수 있는 가능성은 그만큼 더 커진다. SSID는 주기적으로 변할수 있으나 매 사용자는 새로운 ID에 대하여 통보를 받고 무선 NIC를 다시 구성하여야 한다.

유선등가사적비밀보호(WEP)

802.11b표준은 의뢰기들과 접근점들사이의 암호화된 통신을 WEP를 통하여 보장한다. WEP하에서 주어 진 접근점사용자들은 종종 같은 암호화열쇠를 공유한다. 구내에서 이동성을 위하여 모든 접근점들은 동일한 건을 리용하도록 설정되여야 하며 모든 의뢰기들은 또한 동일한 암호화열쇠를 소유하여야 한다. 또한 자료머리부는 해신되여 누구든지 자료전송의 원천과 목적지를 알수 있게 된다.

WEP는 40bit RC4로부터 128bit RC4를 리용하는 약한 규약이다. 그것은 계산상 효과, 자체동기화 및 전송을 위한것이였다. 이런 특성들은 WEP를 마비시키는 특성들이다. WEP에 쉽게 가할수 있는 몇가지 공격들을 아래에 제시한다.

- 통계적분석에 기초하여 전송흐름을 복호화하는 피동적공격
- 알려 진 평문에 기초하여 비법이동국들로부터 오는 새로운 전송흐름을 주입하는 능동적공격
- 약 하루분량의 전송흐름을 분석한후에 모든 전송흐름의 실시간자동복호화를 하게 하는 사전구축공격

대부분의 판매업체들은 WEP가 있거나 없는 모형들을 제공하지만 일부 판매업체들은 우의 제한성들로 하여 WEP를 실행하지 않는다. WEP를 전혀 리용하지 않거나 WEP의 리용을 항상 요구하도록 접근점을 구성할수 있다. WEP를 항상 리용하게끔 접근점을 구성하는 경우에 의뢰기에는 암호화비용이 보내여 지게 된다. 의뢰기가 정확하게 응답할수 없으면 접근점리용이 허락되지 않게 되여 WEP열쇠가 또하나의 통과암호로 된다. SSID를 통과암호로 리용하는 경우와 같이 관리자는 WEP열쇠를 흔히 하는 방법대로 바꿀수 있다. 그러나 같은 의뢰기이므로 통보 및 구성이 문제로 될것이다.

물론 WEP열쇠를 가지고 있는 공격자는 무선전파로부터 파케트들을 엿보기하여 복호화할수 있다.

인증해결책

일부 판매업체들은 인증 또는 범위성문제에 특허적해결책을 제공한다. 무선의뢰기는 접근점으로부터 인증을 요구하며 접근점은 RADIUS봉사기에 그 요구를 보낸다. 인증을 받으면 RADIUS봉사기는 진행중의 대화에 대한 유일한 암호화열쇠를 접근점에 보낸다. 접근점은 그것을 의뢰기에 전송한다. 이 표준은 공유된 열쇠문제의 해결책을 제공하는 한편 흔히 그 해결책은 해당 기관이 한 판매자로부터 모든 설비를 구입할것을 요구한다. 다른 판매자들은 공동열쇠암호기법을 사용하여 매 대화당 열쇠들을 생성한다.

이 인증해결책은 802.1x잠정표준안을 실행하는것과 류사하다. 이 잠정안이 실현되면 판매업체호상간 호환성해결방법으로 이 문제는 결국 풀릴것이다. 802.1x표준은 802기술전체를 위한 일반목적접근조종방식으로 개발되고 있다. 인증방식은 RADIUS의 확장가능인증규약(EAP)에 기초하고 있다. EAP는 의뢰기로 하여금 인증봉사기와 인증규약을 교섭하게 한다. 또한 802.1x표준은 접속암호화열쇠가 변경되도록 허용한다. 이 표준은 빨라서 2002년에 무선제품들에서 나타날수 있을것이다. 관리자는 802.1x를 기다리는 한편 무선 LAN의 보안성을 높이기 위하여 취할수 있는 몇가지 다른 방도들도 가지고 있어야 한다.

제3자제품

무선LAN들의 보안을 보장하는데는 여러가지 제품들이 있다. 실례로 WRQ회사의 NetMotion(www.netmotionwireless.com)은 Windows NT를 통하여 인증되는 사용자가입을 요구한다. 이 회사는 WEP보다 더 좋은 암호화(3DES와 Twofish)를 사용하며 무선망카트접속을 원격으로 사용중지시킬수 있는 능력을 제공한다. 이 해결책과 관련한 중요한 문제의 하나는 봉사기는 흔히 Windows NT에서 운영되여야 하며 의뢰기지원은 오직 Windows 95, 98, ME/CE에 제공되여야 한다는것이다. Windows 2000봉사기와 의뢰기에 대한 지원은 지금 개발중에 있다.

관 문 조 종

관문해결책은 무선통화를 위한 특별부분망을 창조한다. 이 부분망들은 정상경로기들을 리용하지 않고 관문을 가지고 거기에서 인증을 받은 다음에야 파케트들에 경로를 조정해 준다. 부분망들은 IEEE 802.1Q표준을 리용하는 VLAN기술에 의하여 창조될수 있다. 이런 표준에 따라 관리자들은 각이한 교환기에서 선택포구들을 묶어 하나의 부분망으로 결합시킬수 있다. 교환기들이 지리적으로 떨어 져 있다고 하더라도 VLAN중계가 간섭교환기들에서 지원되는 한 이런 결합은 가능하다. VLAN포구들을 리용하는 마디들은 그 다른 부분망들이 VLAN포구인 동일한 물리적교환기에 놓인다 하더라도 경로기나 관문을

지남이 없이는 다른 부분망들에 있는 주소들에 접근할수 없다.

VLAN이 이루어 지면 관리자들은 오직 승인된 사용자들로부터 오는 전송흐름만을 통과시키는 관문을 창조할 필요가 있다. VPN봉사기의 기능이 끌점을 요구하는것이기때문에 VPN관문을 리용할수 있다. VPN봉사기를 관문으로 리용하는것은 턴넬끌점의 인증을 요구할뿐아니라 턴넬에 유일한 건으로 무선흐름을 암호화하여 WEP의 공유된 건을 사용할 필요를 없앤다.

그러나 VPN방법은 리상적이 못된다. VPN의 리해, VPN관문의 선택, 봉사기의 구성과 의뢰기의 지원은 일반LAN관리자가 수행하기 어려운 복잡한 과업들이다.

현재 Georgia Tech가 리용하고 있는 또하나의 해결책은 특수한 방화벽관문을 리용하는것이다. 이 방법은 VLAN을 리용하여 하나의 관문에로 무선전송흐름을 집합하는 방법이다. 그러나 이 관문은 VPN이 아니라 특수화된 코드를 실행하는 이중홈UNIX봉사기이다. Georgia Tech의 IT관계자들은 최근의 Linux핵심부에서 IP표방화벽기능을 리용하여 파케트려과를 보장한다. 접근을 허락하기 위하여 의뢰기는 Web열람기를 열어야 한다. 의뢰기의 HTTP요구에 따라 관문으로부터 자동방향변경인증페지가 열리고 인증요구에 따라 Kerberos봉사기에 보내진다. 인증이 성과적이면 PERL대본은 규칙파일에 IP주소를 추가하여 그것을 IP표방화벽공정에 대한 《알려 진》주소로 되게 한다.

사용자의 관점에서 보면 그들은 열람기를 시동하고 사용자식별기호와 통과암호를 주입하여 망에 접근해야 한다. 의뢰기설치나 인증은 요구되지 않는다. 물론 이 방법은 암호화가 아니라 오직 인증만 보장하므로 수백명이상의 동시사용자들에 대해서는 규모조절을 하지 못할것이다. 이 해결책은 의뢰기에 그 어떤 변화도 주지 않으면서 완전한 작동중 망접근을 허용한다는 점에서는 유일하고 훌륭한것이므로 많은 판매업체의 망기판들을 지원한다. 이 구성은 공통VLAN응용(비행장, 호텔, 토론회 등)에 매우 쓸모 있다.

결 론

무선LAN에는 몇가지 보안상 문제점들이 있어 매우 민감한 망에는 쓸수 없게 되여 있다. 빈약한 하부구조설계, 승인되지 않은 사용, 도청, 가로채기, DoS공격, 의뢰기체계도난은 모두 분석고찰해야 할 분야들이다. 통신을 VPN으로 둘러 싸거나 창조적인 해결책을 개발하면 이런 위험들을 완화시킬수 있다. 그러나 이것은 복잡할수 있다. WEP표준의 변화와 무선기술의 새로운 발전은 리용성은 물론 보안성도 개선할수 있을것이다.

제3편
보 안 관 리 실 천

정보체계보안에서 큰 전진이 계속 이루어 지고 있음에도 불구하고 보안관리자들은 다음과 같은것을 계속적인 도전으로 인정하고 있다. 즉

- 조작체계, 자료기지, 응용프로그람 및 인터네트조작기술에서 증가되는 취약성
- 상부로부터의 불충분한 지원
- 주 및 련방의무조항의 증대
- 보안투자자금의 결핍
- 사용자의 의식과 책임관계의 결핍
- 효과적인 보안탐색가능성의 부족
- 보안이 기업의 창발성의 성과를 담보할수 있다는것을 종종 보여 줄수 없는것

이 편의 여러 장에서는 변화관리, 방책개발, 위험평가 및 관리, 사용자교육 및 의식화와 같은 원리들을 취급한다.

17장에서 William Tompkins는 보안과 기업과정을 시종일관하게 일치시키는것이 가지는 중요성을 상기시키고 있다. 기업사용자들은 자기들의 체계나 응용프로그람이 그들의 요구를 만족시키지 못한다는것을 뒤늦게 알고서는 실망한다. 훌륭한 보안관리자는 기업동업자와의 초기토의에 참가하는것, 기업요구를 수집하는것, 다음에는 그것을 보안요구에로 전환시키는것의 중요성을 인식하고 평가한다. 기업사용자들은 기능성요구를 보장할수 있다. 그렇지만 보안관리자의 임무는 접근조종의 수집, 부호화, 시험 및 실현과 사용자식별, 인증, 검열통제 등이다.

이 편에서는 정보재산보호에 관한 방책에 따라 보안프로그람의 기초를 쌓는것이 가지는 중요성에 대하여 언급한다. 특히 몇개 장은 위험이란 무엇이며 위험을 어떻게 처리하여 정보체계에서 요구되는 신용과 보험을 개발하겠는가 하는것을 취급한다.

기관의 사용자들은 정보담보의 획득과 관리의 주요구성부분으로 된다. 보안관리자가 기업규모의 계속되는 효과적인 보안의식화깜빠니야를 벌리지 않는다면 가장 훌륭한 정보보안방책은 은을 내지 못할것이다. 양성전문가들은 잘 작성된 프로그람은 근본적인 문제들을 고려해야 한다고 한다. 그런 중요한 문제들에는 양성대상의 구성, 청강자들이 정보를 접수하는 방법 그리고 어떻게 그들로 하여금 배운 지식을 기억하고 적용하게 하겠는가 하는 문제들이 속한다. 이 편에서는 가장 우수한 의식화과정의 작용에 대하여 언급하게 된다.

구성관리는 보안실행에서 일관성, 완벽성과 엄밀성을 지원한다. 이 편에서 토론하게 되는 구성관리는 도입되고 있는 기술, 처리, 실천과의 비교속에서 기관의 현재보안자세를 결정하는 방법을 보장하며 보안자세에 대한 변화의 영향을 평가한다.

제１７장. 경영진의 공약유지

윌리암 톰킨스

정보보안, 재해복구 및 비상대책실행자들은 자기들의 제출안을 계획화하여 현실에 도입한 성공의 기쁨을 느끼게 되면 인차 또하나의 더 힘든 문제 즉 자기 기관의 계획을 지속적으로 《혈기왕성하여》 추진시켜야 하는 어려운 파업을 수행하지 않으면 안된다. 더 정확히 말하여 그들은 기업의 지속적운영과 정보보안을 계속 활성화하고 효과성을 높이기 위하여 애쓰고 있는것이다.

많은 경우 힘든것은 경영진으로부터 초기투자획득을 이끌어 내는것이다. 그러나 이 《학과과정(《경영진의 투자획득 제1장》도 볼수 있다.)을 통과》하면 보다 더 힘든 장기적인 과제 즉 경영진의 공약을 유지시키는것이 과제로 나선다. 이 《학과과정)을 《경영진의 투자획득 제2장)이라고 부를수 있다. 이 장에서는 초기투자획득이후에는 무엇을 해야 하는가 하는 문제를 다루지만 초기투자획득의 일부 원리들에 대해서도 폭넓게 다루려고 한다.

이 장에서는 또한 경영진이 관심을 가지고 관리에 참가하도록 하며 경영진의 구입과 승인에 대하여 모든 직원들이 다 알도록 하는 방도들에 대하여 언급한다. 이 프로그람들의 끊임 없는 성공을 위한 중요한 요구의 하나는 관리에 대하여 잘 알고 공약화하도록 하는것이다. 경영진이 프로그람을 잘 지원하지 않는다면 다시 말하여 경영진이 프로그람에 대한 지원이 중요하지 않다고 생각하는 경우에는 다른 종업원들이 그 사업에 참가하지 않게 될것이다.

《최근에 당신들은 나를 위해서 무엇을 하였소？》

지금까지 몇명의 실행자들은 그들의 경영자들로부터 이런 말을 듣기는 하였지만 대부분의 실행자들은 이런 말을 경영자들에게서 듣지 못하였다. 그러나 많은 경우에 많은 경영자들은 이런 프로그람을 하나의 개발계획으로만 생각하는것은 사실이다. 즉 경영자는 《이 개발계획이 완성되면 나는 다른 더 중요한 개발계획을 해야겠다.》고 생각한다. 이렇게 놓고 보면 정보보안 및 재해복구계획자들은 언제나 마음이 편안치 못하다. 실행자들이 계속 강조해야 할 중요한 조항은 목표인것이 아니라 려행이라는것이다.

이런 려행은 무엇을 포함하는가. 이 장에서는 아래의 4개 항목들에 주목한다.

- **의견교환** 우리가 어떤 의견을 교환하려고 애쓰고 있는가. 우리는 누구와 의견교환을 하고 있는가. 우리는 그들이 어떤것을 들었으면 하는가.
- **만나기** 실행자는 언제나 경영자들과 만나게 될것이다. 그러니 우리가 만나는 각이한 수준의 경영자측에 무엇을 말해야 하는가.
- **교육** 경영자를 포함하여 모든 사람들에 대한 교육은 계속되는 공정이다. 경영자가 배워야 할 정보는 어느정도인가.
- **고무** 경영자를 고무격려하고 그들을 계속 지원하려면 어떻게 해야 하는가

통 신

경영자와 대화하기가 왜 어려운가. 《경영자는 실행자가 요구하는것을 리해하지 못한다.》, 《경영자는 오직 비용에 대하여 근심할뿐이다.》다시 말하여 《경영자는 의견을 들으려 하지 않는다.》이런 생각들은 실행자들에게 익숙해 진 생각이다. 전달내용은 경영자의 마음에 그대로 새겨 져야 한다. 그러나 여기서 중요한 문제들은 다음과 같은것들이다. (1) 실행자들은 현실에 발맞추어야 한다. (2) 실행자들은 경영자들이 기업에 대하여 리해할수 있도록 말해야 한다. (3) 실행자들은 비용절약안들을 생각해 내야 한다(이 안자체가 일정한 일을 필요로 할수도 있다.).

가정과 현실

의견교환해야 할것과 의견교환하지 말아야 할것은 무엇인가. 둘다 중요하다. 그러나 보안과 기업련속운영에서 가정을 피하는것은 사활적이다. 관리와 보안/BCP(기업련속계획)실행자들이 부정확한 가정의 후과로부터 손실을 당하는 실례는 많이 찾아 볼수 있다.

재해복구계획분야에서는 상급경영자가 기관의 실제적인 회복능력을 알도록 하는것이 무엇보다도 중요한것이다. 경영진은 기관에서 재해가 일어 나는 경우 현실적으로 복구가 최소한 며칠이 걸림에도 불구하고 몇시간내에 인차 회복할수 있을것이라고 쉽게 가정할수 있다. 현실적으로는 기관의 각 부서들이 기관전반의 재해복구를 념두에 두지 않고 오직 부서의 자그마한 망설비와 부분망설비만 구입하여 설치하지만 경영진은 이 각 부서들이 재해복구조정관의 주관하에 서로 협동을 잘해 가면서 재해복구계획을 잘 집행하고 있다고 가정하는것이다. 또한 재해의 심각성이 얼마나 큰가에는 상관없이 모든 정보가 재난이 일어 나기전 시간의것으로 환원복구될수 있다고 생각하지만 현실적으로는 그 전날밤의 예비본까지로밖에 복구할수 없으며 더우기는 며칠전의 수준으로도 될수 있는것이다.

이렇게 되면 가정을 잘못한 후과가 오게 된다. 2000년 3월 어느 한 보안대회에서 Global Integrity회사의 유진 슐쯔박사는 어느 한 유명한 정보보안전문가에 대한 이야기를 하였다. 이 전문가가 상당히 훌륭한 보안계획을 가지고 있다고 생각하였는데 사실인즉 이 전문가가 회사의 기업과정에 대한 실상을 잘 파악하지 못하고 그 계획을 작성하다보니 자기네 회사의 상급경영진은 그 보안계획에 실망을 느끼고 말았다는것이였다. 이렇게 실망하게 되면 경영진이 그 계획에 대한 투자가로서의 지위를 잃게 될수도 있고 예산상 지원도 받지 못할수도 있으며 잘되는 경우에도 경영진이 그 계획개발과정에 자기들이 참가하지 말아야 되겠다고 생각하게 되는 정도까지 그 후과가 이르게 될것이다.

각이한 관리수준에는 각이한 방법을

어느 기관이든지 실행자가 어느 기관과 의견교환을 해야 하는가에 따라 주의할 문제가 결정되며 토론할 문제는 반드시 경영자가 리해할수 있는 말로 이야기되여야 한다. 기술적인 술어로 마구 말하지 말아야 한다. 다시 말하여 그들이 기억할수도 없는것 그리고

지어 알려고도 하지 않는것을 가르치려고 하지 말아야 한다.

이야기분야에서 리해력을 높이기 위하여 실행자가 사용하는 참고서는 경영자들이 쓰는 말로 즉 경영자들이 알아 들을수 있는 말로 해석해 주어야 한다. 가능하면 원가상 리득 및 원가회피방책들과 기관의 계획작성 및 계획관리의 한 부분으로 될수 있는 기업성사요인들과 같은 기본기업방책들에 의거하라. 비상대책계획화봉사 혹은 정보보안자문이 기관의 업무가 아닌 경우 회사가 BCP 혹은 InfoSec로부터 어떻게 수입리득금을 얻을수 있겠는가 하는것을 보여 주기 어렵게 된다. 그러나 얻게 될 리익에 대하여 그리고 BCP와 InfoSec가 시작부터 MIS계획작성에 포함되는 경우에 피할수 있는 엄청난 비용에 대하여 항상 토론할 준비가 되여야 한다.

표 17-1　　원가상리득과 원가상회피

	BCP	Inf Sec계획
편의		
기관에 대한 보호	○	○
회사의 명성유지	○	○
리용성의 담보	○	
부주의로 인한 보안위반의 최소화		○
고의적보안침해에 대처한 노력의 최대화		○
취소		
계획에 없던 복구원가의 증대	○	
이미 완성된 응용 또는 체계에 InfoSec(또는 BCP)를 추가하기 위한 총계획비용의 4배(혹은 그이상)증가	○	○
기업을 그만두는 경우에 드는 비용…?	○	○

표 17－1은 대부분의 회사들이 인정할수 있는 원가상 리득과 원가회피(투자후 효과에 비하여)의 간단한 몇가지 실례들이다.

실행자들은 … 기업을 살리는 사람들인가

기관은 《전형적인》회복태세를 갖추지 못하고 있다. 즉 정보기술회복계획은 작성되나 기업공정회복은 계획화되지 않는다. IT계획에 대한 요구가 어떻든지간에 실행자는 집단의 쓸모 있는 성원으로 인정 받기 위하여 그리고 의의 있는 요인들(기업공정들이 계속 진행되여 나갈수 있게 하는)이 계획의 초기개발단계에서 고려되도록 하기 위하여 계속 노력하여야 한다. 실행자들이 경영자의 가정에 의거하지 않으며 회복(있을수 있는 최대정전지속시간), 체계실패탐색, 가동기간담보(내적 및 외적), 성능지표 및 봉사수준가격모형들과 같은 명백한 회복봉사수준항목들을 토의하고 문서를 제공할 때 실행자들은 기업

추동자로 인정될것이다.

오늘의 기업세계에서 거의 모든 기업들이 인터네트에 일정하게 의존하게 될것이라는 것은 일반적인 사실이다. 기업공정들의 성과는 회사가 자동화된 기업공정을 실시간에 얼마나 빨리 회복시키거나 복구하는가에 크게 의존된다는것을 알려 주는것은 사활적인 요구로 되였다. 이런것을 성과적으로 통보할 때 그 기관의 손실들과 동업자들이 그 회사에서 보장하는 안전수준을 높이게 된다. 그것은 안전수준이 회사가 얼마나 효과적으로 망으로 련결된 기업공정을 조종하는가 하는것을 보여 주기때문이다.

《새로운》체계개발에 일찌기 인입되여야 한다. 기업공정의 초기개발단계들에서 고려되는 정보보안 및 사고방지계획을 위한 방책적요구를 세우기 위하여 필요한 대책을 세우는것은 절박한 문제이다. 이것들은 보충비용이 아니라 하부구조비용의 일부라는것을 강조하여 주어야 한다.

IT관점에서 출발하여 새로운 기입공정개발을 추동하려는 현 추세를 따르지 말고 새로운 기업공정에 기초하여 IT보안을 추동해야 한다. 즉 자동화된 기업공정들이 기업상 요구에 기초하여 그 구조가 형성되여야 한다.

해당한 사람들을 만나라

언급된바와 같이 회사의 조직체계에서 실행자가 어느 자리를 차지하고 있는가에 따라 누구와 함께 일을 시작할것인가 하는것이 결정되게 될것이다. 그러나 우선 (1) 기업을 알아야 하며 (2) 경영자가 무엇을 바라는가를 알아야 하며 또한 (3)기술적요구사항들을 알아야 한다. 실행자들은 행정관리가 어떻게 《움직이는》가에 대하여 미리 알아야 한다. 그렇지 않고 설계단계에서 틀림없이 사멸될 안을 밀고 나가려고 한다면 아마도 그것은 소득보다 오히려 손실을 더 당하게 할것이다(표 17－2를 볼것).

표 17－2　　　　소 개 모 임

새로운 기관에서 사업을 시작하면서 내가 스스로 맡은 가장 중요한 과업의 하나는 될수록 많은 경영자들과 일대 일로 만나게 되는 《소개모임》을 시간표화하는것이다. 이 모임을 설정하게 된 목적은 기업을 알자는것이다. 나의 역할을 토론하자는것이 아니라는것을 모든 경영자들에게 말해 준다. 그것은 나의 역할이 아직 형성단계에 있기때문이다. 나의 역할을 수행하기 위하여 그 부서의 기업공정에 대하여 내가 알 필요가 있다는것을 미리 그들에게 말해 둔다. 내가 기업공정을 배우는데 정말 흥미를 가지지만 그 부서의 IT사용에 대해서는 그닥 흥미를 가지지 않는다는것을 그들에게 인식시켜야 한다. 다음으로 나는 그들에게 기관에서 어느 사람을 만나야 그 기관에 대한 더 완전한 표상을 내가 가질수 있겠는가고 물어 보면서 그런 사람을 소개해 주지 않겠는가고 부탁한다(그다음부터는 그들의 권고에 기초하여 사람들을 만난다.). 마지막으로 가능하다면 그들이 보안성에 대한 우려를 가지고 있는가 하는것을 나는 물어 본다. 나는 이 첫 모임을 약 반시간정도로, 야외에서라면 기껏해서 45분 넘지 않게 하려고 한다. 높은 경영자들에게서는 기껏해서 15분이나 《짜내》겠는지…. 어쨌든 가능한껏 시간을 내서 이야기하라.

실행자가 항상 잊지 말아야 하는 몇가지 가장 중요한 문제들은 다음과 같은것들이다.

- 경영자가 우려하는것은 무엇인가.
- 조직사업을 하여 수행할것은 무엇인가.
- 나는 무엇을 도울수 있겠는가. 장기적인 전략계획을 토의하기 위하여 준비된 어떤 회의에도 참가하라. 단기적인 전술적사업토의에 준비되여야 한다. 있을수 있는 예산요구를 토의할수 있게 언제나 준비되여야 한다.

실행자관리공약강령의 항목들중 하나를 다시 강조하면서 실행자들은 기술변화와 관련하여 자신들을 현실에 발맞추어야 한다. 기관이나 회사에 미치는 정보기술영향에 관한 토의에 준비되여야 한다. 표 17−3에는 실행자가 알아야 할 몇가지 항목들이 소개되였다.

행정관리의 측면에서 실행자는 보안방책토론에서 항상 허심해야 한다. 방책을 작성하거나 수정하는것은 실행자가 관여하는 가장 신중한 문제들중의 하나이다. 방책작성이 실행자의 특정한 권한에 속하는것은 아니지만 실행자는 의견을 제기하며 자기의 경험에 기초하여 방책초안을 작성하게 된다. 또한 실행자는 방책작성권고에서 집단이 존중하는 성원이다. 특히 회사는 방책에 대하여 정기적으로 검토하는가, 어떤 수준에서 그 복잡한 구체적인 내용들이 기관의 방책에 반영되는가, 실례로 방책은 누구에게 의무 또는 책임이 있는가 하는것을 규정하는가, 방책이 그 준수를 제기하는가 즉 방책이 못을 때리는 《마치》를 가지고 있는가, 방책이 어떻게 실행되는가 등. 실행자는 방책의 각이한 수준 례컨대 높은 수준(정보원천보호)과 보다 구체적인 수준(WWW의 리용방책 혹은 Web싸이트회복절차)을 구별할수 있어야 한다.

표 17−3　　　토의제목들

다음의것을 토의할 준비를 하라 :

- 총 회복비용
- VAN상의 EDI로부터 VPN에로 이동
- 총 운영가격
- IP상에서의 음성전송
- 음성인식체계
- 무선통신망구축
- 자체복구적인 망
- IT위험보험
- 자료보관고구축의 효과
- 값되물기계산
- BCP와 InfoSec의 개념화
- 가상경로기의 여유규약

행정관 및 상급경영인과의 만남 실행자들은 집행위원회의정토의에 참가할 준비가 되여 있어야 한다. 이런 기회들이 있게 되면 자신들을 잘(혹은 나쁘게) 보일수 있다. 무엇이 수행되였는가, 무엇이 발생하고 있는가 그리고 무엇이 진행되고 있는가와 같이 중요한 문제를 알기 쉽게 간단히 말해야 한다. 또한 기관의 생산부문에 해당한 정보와(계획된) 제출현시안(presentation)을 간단하게 준비하는것이 중요하다는것은 두말할 필요조차 없다. 알기 싫어 하고 기억할수 없는것을 경영자들에게 알려 주기 위하여 애 쓰지 말아야 한다는것을 명심하라.

중간수준경영자들과의 만남 그들과 지난번에 만난 이후 일이 어떻게 달라 졌는가에 대하여 주의를 집중하라. 경영자들의 견지에서는 자기 기업문제에서 무엇이 달라 졌는가, 실행자의 견지에서는 지속 및 보안활동에서 무엇이 변하였는가, 나타난 변화들로 하여 회복 혹은 보안우선권에서의 모든 변화들을 토론하게 하라.

기관의 인사부성원들과 좋은 관계를 맺는것이 아마도 중요할것이다. 한가지 리유는 회사의 신입사원지도요강에 정보보안소개의 도입을 추진시키자는것이다. 또 한가지 리유는 기관의 《새》경영자들에 대하여 알도록 하자는것이다. 오늘의 종업원이 언제 경영자의 지위로 승진되는가 하는것을 알아 내는것도 또한 중요하다. 보다 중요한것은 기관밖의 성원이 언제 결원된 경영자의 자리를 차지하는가를 알아 내는것이다.

교 육

지속교육프로그람은 이것이 도달목표가 아니라 진행과정이라는 또하나의 훌륭한 실례이다. 누구나 기업공정에서 거의 계속되는 변화들과 기업공정을 지원하는 기술에 맞다들게 되므로 기관의 모든 종업원을 계속 교육하는것이 얼마나 중요한가 하는것을 누구나 알수 있다. 비록 힘겨운것 같기는 하지만 현대기술에 의하여 발생된 취약성과 비밀의 로출로 인하여 자기의 회사와 자신을 갱신해야 한다는것을 다시 한번 강조해야 한다.

실행자는 신간업계잡지들을 읽어야 한다. 기업지속 및 정보보안잡지들뿐아니라 기관산업과 관련되는 업계잡지들을 읽어야 한다. 교육사업을 지원하는 잡지기사들은 언제나 들고 다니면서 기업관리에 리용될수 있게 준비해야 한다. 또한 실행자는 회복이나 보안과 직접 관련된 기술의 변화에 대하여 경영자들에게 알려 주어야 한다. 이 기사들은 주로 중간수준의 경영자들이 읽도록 하는것이 여기서는 필수적이다. 책임경영자는 우선 문제를 제시하고 보충정보에서 그 문제가 노는 역할에 대하여 명백하게 리해해야 한다. 그 다음에 상급경영자들에게 지원문건(기사 등)을 제공하는것이 가장 효과적이다.

또하나의 《교육》형식은 전자우편경로를 통하여 실현하는것이다. 파업을 계획하는 InfoSec 혹은 BCP와 관련된 기관안내전자우편을 보낼 때에는 해당한 경영자들에게 복사본을 보내라.

위험관리주기(그림 17－1)에 대한 토론(검토)에 준비되여 있어야 한다. 즉 실행자가 《이 계획은 완성되였다.》라고 말해야 할 때가 올것이다. 실행자는 위험관리주기에 대하

여 어느때이든 빨리 요약할수 있게 준비되여 있어야 한다.

1단계 기관의 환경 혹은 재산을 정의 혹은 갱신하라.
2단계 기업영향 혹은 위험분석을 수행하라.
3단계 기관의 현 운영상태 그리고 재산에 대한 영향에 기초하여 방책, 지침, 표준 및 절차를 개발 혹은 갱신하라.
4단계 회사의 임무와 목적을 지원하는 방책 등을 강화하기 위하여 체계 또는 공정을 설계하고 실현하라.
5단계 그 체계들을 행정적으로 실현하고 유지하라.
6단계 체계와 기업공정을 시험하며 그것들을 검열하고 그것들을 탐색함으로써 바라는 목표를 달성할수 있게 하라. 그리고 시간이 흘러감에 따라 이 주기는 반복되여야 한다. 바로 이때 모든것이 변하였으며 회사가 환경과 자기 재산을 재평가할 필요가 있다는것이(탐색, 시험, 검열을 통하여) 결정된다.

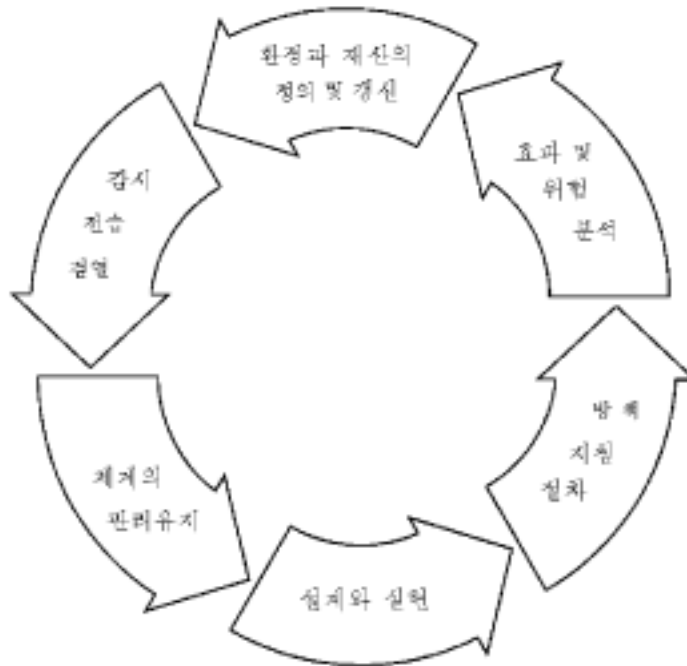



그림 17－1. 위험관리주기

대부분의 회사들은 년간 및 반년간의 종업원회의들을 말단수준(실례로 부서모임)에서 정기적으로 가진다. 실행자는 이런 회의들의 의정에 상정될 중요한 항목들을 장악해야 한다. 실행자들은 될수록 기관안에서 인정을 받아야 할 문제들을 항목으로 설정하여 의정에 제기하게 된다. 그렇지 않으면 최소한 경영자들이 종업원들에게 말하려고 할 때 그들에게 이런 항목들을 보장하라고 요구하여야 한다.

경영자의 책임성

실행자는 경영자에게 다음과 같은 정보(교육)의 일부 항목을 제공할 시간을 구체적으로 선택하여야 한다. 그러나 여기서는 다시 지속/보안프로그람의 성과여부가 경영자의 리해와 지원에 좌우된다는것을 강조할 각오를 해야 한다.

- 모든 종업원들이 기관의 어떤 자원에 접근하기에 앞서 IT사용자의 책임성을 알도록 하는것
- 솔선수범: BCP 혹은 InfoSec제안에 대하여 적극적으로 눈에 띄게 지원하는것
- 정보를 보호하고 방책을 개선하는 사람들에 대한 평가와 보수(경영인이 이런것을 하려고 하지 않는다면 적어도 실행자들이 그것을 하게 허락하도록 납득시키라.)

모든 종업원들을 망라시킬 때 그것이 경영자의 교육에 주는 영향을 스쳐 보내지 말라. 프로그람에 종업원을 망라시키는 사업을 장려하여야 한다. 자기들의 참가가 정보보안 및 회복프로그람의 성과에 의의 있는 요인으로 된다는것을 알면 종업원들은 의식을 크게 높이게 될것이다. 종업원들은 자기들이 기관에서 중요한 역할을 한다는것을 인식하게 될것이다. 그러나 무엇보다도 중요한것은 말단단위의 종업원들부터 올라 가면서 먼저 프로그람보장사업에 참가시키는것이다. 경영자가 회복 혹은 보안문제들에 대하여 종업원들로부터 듣게 될 때 그들은 회사를 위한 사업에 관심(보다 큰 관심)을 가지게 될것이다.

추 동 요 인

여기서는 경영자들을 행동에로 추동하는 문제들 즉 적어도 경영자들이 지속적회복 및 정보보안계획과 반복적인 사업들을 지원하도록 추동하는 문제들에 대하여 재학습하게 된다.

일부 사람들은 관리자를 추동하는 주요요인이 돈이라고 한다. 기관의 소득이 높아지면 경영자들은 흔히 기뻐한다. 반대로 기관에 재정적부담을 주고 투자에 대한 리윤을 기대할수 없는 경우에 경영자들은 훨씬 더 신중해 질것이며 사업에 대한 평가와 인정을 하려는 용기가 나지 않게 될것이다. 재정문제외에도 경영자들이 기업지속 및 정보보안계획을 지원하도록 추동하는데는 여러가지 방도들이 있다. 그러나 가장 많이 사용된(그리고 람용된) 방법은 FUD(두려움, 불확신 및 의심)이다. FUD는 더 구체적으로 보면 고위당국의 지시나 명령의 측면들, 례로서 회사의 관리리사회 혹은 주주들의 명령을 들수 있다.

보충적으로 법적, 조직적 및 계약적의무에 응해야 할 요구들은 경영인들에게 더 큰 인상을 주는것이다. 관리의 견지에서 적극적인 요인으로 되는것은 생산성을 높이는것이다. 생산성이 높지 못한 경우에는 적어도 정보보안과 기업사고방지계획이 생산의 정상화에 도움이 되리라는 확신이 그런 추동요인으로 된다. 다행히도 많은 실행자들은 관심을 불러 일으키는 추동요인들을 성과적으로 리용하기 시작하였다. 다음 부분들에서는 구체적인 추동요인들과 함께 모든 추동요인들을 고찰하게 된다.

FUD 즉 두려움, 불안 및 의심

경영자의 관심을 가장 빨리 끄는것중의 하나는 불행한 일이 발생하는것이다. 례컨대 이웃사무소건물에서 일어 난 화재 혹은 새로운 비루스의 발생과 같은것이다. 표 17－4에서는 2000년에 일어 난 몇가지 주요사변들을 보여 준다.

표 17－4 현실적으로 일어 났던 FUD실례들

회오리바람	3월 28일 오후 6시 텍싸스주 포구워스 중심거리; 3월 28일 비상대책성원들이 건물들을 조사하고 구조물파괴상태를 결정할 때까지 중심지를 차단.
하리켄(열대성 폭풍의 일종)	9월 17일 오후 플로리더주 탬퍼만의 고던. 폭풍과 큰물.
화재	5월 12일 뉴멕시코주 로스알라모스. 산림봉사대 공무원들에 의하여 화재가 발생하였다. 계획적인 활동으로 화재를 제거…. 1만 1천명의 시민들이 소개되였다(2000년 5월 15일 AP통신).
테로	여러건, (1) 아랍해커들이 미국과 이스라엘에서 유태인Web싸이트들에 많은 공격을 하였다. (2) 파키스탄그룹들이 인디아 등지에 있는 Web싸이트들을 정기적으로 공격하고 있다.
정탐	QUALCOMM회사사장은 전국회의참가중 호텔회의실에서 무릎형콤퓨터를 도난 당하였다. 무릎형콤퓨터에 있는 QUALCOMM비밀정보를 획득하는것이 목적이였다고 추측되고 있다(2000년 9월 11일 AP통신).
사회적영상	(혼란) 9월에 Web싸이트수리중 해커들이 웨스턴 유니언 Web싸이트를 리용하는 사람들에게 속하는 1만 5천개이상의 신용 및 차방카드수자들을 전자복사하였다(2000년 9월 11일 AP통신).

식초보다 꿀로 파리를 잡는것이 더 쉽다

수많은 FUD의 실례들이 있지만 실행자들은 경영자들의 지지를 따내기 위한 하나의 수단으로서 FUD를 리용하는데서 주의해야 한다. 《승냥이다!》라고 소리만 지르는 사람이 아니라 해결책들을 제공하는 능수로 되여 신뢰를 받는 능력 있는 사람으로서 실행자가 인정을 받게 될 때 비로소 경영진의 공약이 더잘 유지될수 있을것이다. 가령 FUD를 유리하게 사용할 적당한 때라든가 경영자에게 제출할 FUD의 실례가 없다면 우선 정보보안 혹은 기업비상대책계획에 대한 경영자의 지원도 없게 될것이다.

아마도 경영자들에게서 FUD에 대한 가장 걱정스러운 측면은 사회적불안인것 같다. 출판물의 혹평 다시 말하여 회사이름을 신문제목에 불리하게 싣는것은 경영자들이 피하려고 적어 놓는 첫 항목이다. 실행자는 사회적불안과 회사의 중요한 성과자료의 핵심적

인 한몫을 로출시키는것을 극복하는 문제를 훌륭하게 돕기 위하여 모든 주요정보기술계획에 의무적으로 참가하게 된다. 믿음직한 접근관리조종과 자동기업공정에 대한 신속하고도 효과적인 회복력량도 계획화하여야 한다. 기관안에서 정보기술지원을 받는 기업공정을 개발하거나 개조할 때 접근조종 및 회복계획은 모든 계획에 의무적으로 포함되여야 한다. 각이한 기관들은 중요한 성과자료를 결정하는 각이한 기준들을 가지고 있다. 경영인들이 종종 고려하게 되는 문제는 회사가 자기의 중요한 성과자료를 공개하려고 하는가 하는것이다. 오늘의 발전하는 기술환경에서는 계획개발생명주기의 계획화가 완전하지 못할 경우에는 회사의 중요한 성과자료를 쉽게 고려할수도 있게 된다는것이 현 실태이다.

응당한 관심

오늘날의 기업세계는 기업공정들에 제공되는 지원정보자원에 철저히(거의 완전히) 의존하게 된다. 실행자는 그런 지원정보자원을 보호통제하게 되며 필요한 경우에는 이전자원들을 리용할수 있다는것을 기관에 납득시키기도 한다. 이런 사정으로 실행자는 보호대 사용상 편의, 손실위험 대 보안통제비용의 균형을 효과적으로 맞추어야 할 임무를 맡게 된다. 위험분석공정(주관적인)에 지장을 주는 불일치에 기초한 보호 및 회복성《최소》요구를 경영자들에게 납득시키는것과는 반대로 기관들에서 제기되는 이런 희망들에 대한 리성적인(접수될수 있는) 균형을 결정하는데 응당한 관심을 돌리는것이 보다 생산적이라는것을 많은 실행자들은 알게 되였다.

어떤 회사에서든지 응당한 관심이라는 고려항목을 요약한다면 다음과 같다. 경영자들이 (1)보안통제 및 회복계획들이 류사한 기관들에서 보게 되는 그런것들과 비교될수 있게 전개되였다는것과 (2) 그들이 또한 기업지속 혹은 정보보안에 투자를 일정하게 하였다는것을 제시할수 있는가 또한 기관에서 그렇게 하지 않는 타당한 기업적근거를 문건상에 밝혔는가.

법적, 규정적 및 계약적의무조항

일정한 형태의 의무조항이 규정적인 의무조항(증권 및 교역위원회, 련방재정기관심사리사회 혹은 보건재정국)이건, 법적의무조항(1996년 보건보험공용 및 책임관계법, IRS 기록보존법 그리고 각이한 주 및 련방 콤퓨터보안 및 범죄관계법)이건, 회사리사회의 지령이건 혹은 검열원보고에 지적된 사항에 기초한 건의안들이건 관계없이 모든 기관들이 다 책임진다. 응당히 집행경영자는 기업에 영향을 주는 규정과 규칙에 대하여 인식하게 해야 한다. 이러한 기업영향에 익숙해 져 있게 되면 실행자는 그로부터 혜택만을 입게 될수 있다. 어느 회사들에서든지 실행자가 이런 규정과 규칙들에 대한 경영자의 리해정도를 파악하고 실행자에게 설명하여 줄 특히 정보기술의 지원을 받는 기업공정의 실현에 그것이 어떻게 영향을 주는가와 관련하여 설명하여 줄 기회가 있을것이다.

모든 실행자들은 큰 정보기술계획의 계약명세서를 작성하는데 참가하거나 혹은 적어도 의견이라도 제출하여야 한다. 기관들은 전자상업거래가 기업을 수행하는 정상적인 한 부분이라는것을 기대하기 시작하였다. 이런 견지에서 모든 기업동업자의 보안 및 비상사

고대책에 대한 보안 혹은 재해복구평가를 외부계약당사자들이 실제로 수행하도록 허락하는 계약상 요구에 직면하게 될수도 있을것이다. 실행자는 회사의 망에 대하여 접수할수 있는 수준의 내부검토를 진행할 준비가 되여 있는가. 실행자는 경영자의 방조자로서 우선 운영환경에 실제적인 보호범위를 정확히 판단하기 위한 요구를 기업동업자들이 계속 확장할수 있게 하며 자기 기관안에서 접수될수 있는 구체적인 계약조항들을 보장할수 있게 준비한다.

생산성

기관이 봉사를 목적으로 한다면 다시 말하여 고객들과 협력자들에게 각이한 수준의 봉사를 보장하려고 한다면 접근조종은 필수적인것으로 된다. 체계개발, 실현 및 유지를 잘하면 오직 해당한 사용자만 그 체계에 접근하게 할수 있고 사용자가 작업하려고 할 때 리용하게 할수 있다.

오늘의 기술적작업환경에서 대부분의 경영자들은 반드시 정보기술과가 최신의 실시간적인 기술대책들을 실시하고 갱신하여 나가야 한다고 주장할것이다. 비루스를 자동적으로 제거하지 않고서는 정보자원의 기관적리용을 할수 없다는것은 의심할바 없다. 비루스방지를 잘하고 갱신하면 종업원들의 생산성은 적어도 안정되게 될것이다.

암호화가 생산성을 높이는가에 대한 견해는 각이하다. 그러나 암호화가 기업을 살린다는것을 부정하는 경영자는 거의 없다. 암호화는 공유되는 통신만이 엑스트라네트이건 인트라네트이건 혹은 인터네트이건 관계없이 그것을 통하여 송신되는 사적비밀에 대한 믿음과 정보의 비밀성을 더욱 확고하게 하여 준다. 기업은 암호화의 비밀성에 대하여 담보할것을 요구하고 있으며 또 계속 요구할것이다. PGP와 수자식서명의 우월성을 리용하는 대렬이 계속 늘어 나고 있으며 비밀엄수를 요구하거나 신속정확성을 요구하는 회사의 정보가 수신인 한사람만이 해당한 정보를 볼수 있도록 신뢰성 있게 공개망으로 송신될수 있는 보다 큰 담보가 이루어 지고 있다.

어떤 콤퓨터사고에도 대처할수 있도록 기관들의 기초기술토대가 마련되고 있다. 적극적이고 믿음직한 대응책을 해결함으로써 기관들에서는 랑비시간을 대폭 줄이고 생산성을 높여 나갈수 있는 확고한 담보를 쌓고 있다.

경영자를 추동하기 위한 협력

실행자들은 검열자가 경영자로부터 신뢰를 획득하는데서 자기들과 동맹자라는것을 느낀다. 그러나 어떤 정황도 검열자의 견지에서 보아야 한다는것을 잊지 말아야 한다. 다시 말하여 모든 임무공정들(지속성공정과 보안공정까지 포함하여)이 무결성이 담보되는 공정으로 되도록 하는것이 그들의 임무라는것이다. 이런 전제는 기업과정의 통제수단들을 개발하기 위한 의견들에 검열자를 인입하려고 시도하게 될 때 리해에서 불일치가 있을수 있다. 그러나 동시에 실행자들이 회사안의 검열성원과 토론하여 협력관계를 조절하려는것은 아주 좋은 구상이다. 내부검열과 보조를 맞출 때만이 기관안에서 성과를 거둘수 있으며 개선할수 있는 문제와 관련한 중요한 정보를 얻을수 있게 될것이다.

또한 실행자는 법관계일군들과 동맹자가 될수 있으며 또 이와 반대로 법관계일군들이 실행자와 동맹자로 될수 있다. 이런 《추동요인》은 이 편람의 이전 판들에서 지적된만큼 이 장에서는 언급하지 않았다.

요 약

경영진의 말 당신은 이것을 자체로 할수 있지요, 당신은 전문가가 아닌가요?

실행자의 대답 이런것은 언제나 협동해야 할 일입니다. 저의 견해에 의하면 저는 아무리 알려고 해도 그 일을 실지 수행하는 사람들만큼 세부적인것을 절대로 할수가 없습니다.

실행자들은 자기들의 1차적인 과제가 경영자의 1차적인 과제로 되게 해야 한다. 그러나 더 중요한것은 경영자의 1차적인 과제가 실행자의 1차적인 과제로 되게 하는것이다. 실행자는 경영자의 우려와 경영자가 어떤 항목에 주의를 돌릴것인가를 아는것이 중요하다.

실행자는 기관안에서 기업촉진자로 인정 받기 위하여 노력해야 한다. 일을 잘하는 실행자는 계획팀의 중심인물이 되여 항상 없으면 안되는 그러한 사람, 그에 의거해야만 충돌문제의 성과적인 해결을 볼수 있는 사람인것이다. 그러한 충돌문제의 례를 들어 본다면 명백히 분할화되고 프로그람적으로 조종화된 효과적인 자동업무공정과 사용자의 사용상 편의와의 충돌을 들수 있다.

《고객은 언제나 옳다.》이렇게 말하는것은 흔히 써오는 에둘러 말하기이다. 그러나 모든것을 고려해 볼 때 이것은 실행자에게 특별한 의의를 가지고 있다. 경영자가 지지할수 없는 결정과 행동을 실행자가 내밀수 있는 정황은 드물다. 실행자가 기업을 알려고 애 쓰고 기관의 기업과정들에 영향을 주는 업계의 변화에 보조를 맞추어 갱신하면 그는 고객이 요구하는것을 알게 될것이다. 즉 실행자는 경영자와의 공약을 유지하는데서 성과를 거두게 될것이다.

제１８장. 보안의식의 계발

쏘즌 디 헨취

정보기술 (IT)은 우리의 일상생활의 모든 면에서 뚜렷이 안겨 온다. 너무도 명백하므로 많은 경우에 그것을 전혀 느끼지 못할수 있다. 전자우편 혹은 육성우편이 없이 기업을 운영한다고 생각해 보라. 손으로 보고서를 쓰고 후에 전자타자기를 리용하여 그것을 타자하면 어떻게 되겠는가. 콤퓨터기술과 공개결속된 통신망은 분야나 기업의 특수한 요구에 관계없이 모든 기관들의 핵심적구성분인것이다.

정보기술은 정부와 사영분야들에서 전례없이 많은 정보량을 창조, 가공, 저축 및 전송을 진행할수 있게 한다. 이 정보흐름을 다루기 위하여 건설된 IT하부구조는 산업운영의 전일적인 한 부분으로 된다. 사실 대부분의 기관들은 자기 기관의 생존이 자기들의 정보체계에 달려 있다고 생각한다. 정보체계에 대한 이런 의존은 사무를 능률적으로 수행하는 기관의 능력을 위험하게 만들수 있는 행동으로부터 하드웨어, 쏘프트웨어와 같은 물리적자산들 그리고 이것들이 가공하는 정보들을 보호하도록 해야 할 필요를 제기하였다.

> 여러 IT보안보고들은 기업이 10여일간 자기 자료에 접근하지 못하면 그것은 경제적손실로부터 재정적회복을 할수 없다고 평가한다.

정보기술은 급속도로 발전하지만 취약성과 위험에 대해서는 사용자들에게 별로 알려주는것이 없다. 1999년 3월 콤퓨터보안연구소소장 Patrice Rapalus는 정보시대에 대처해나가려는 회사들과 정부기관들에서는 정보체계보안전문가들의 채용과 양성에 더 많은 자원을 돌려야 할것이라고 하였다. 이에 대하여 좀 더 보면 정보체계보안전문가들을 더 양성할뿐아니라 정보체계에 접근하는 모든 종업원들이 사용하는 IT체계에 있을수 있는 취약점들과 위협요소들을 잘 알며 그들이 정보보호에 도움을 주자면 어떻게 해야 하는가를 알도록 하여야 한다.

종업원들 특히 IT체계말단사용자들은 일정한 실행에 의하여 생기는 보안결과들에 대하여 누구보다도 모른다. 대부분의 종업원들에게 있어서 IT체계는 될수록 빨리 될수록 효과적으로 작업과제를 수행하는 도구로 된다. 다시 말하여 보안은 필수적인것이라기보다 장애물로 간주된다. 그리하여 정보보호에 적극적으로 참가하지 않을 때 빚어 지는 위험과 결과에 대하여 알려 주는 IT와 관련된 정보를 모든 기관들에서 종업원들에게 보급하는것은 절박한 문제로 된다. 사실 법(1987콤퓨터보안법)은 련방기관들이 정보체계의 모든 말단사용자들에게 보안의식화정보를 보급할것을 요구한다.

종업원들은 IT체계와 그들이 처리하는 정보의 보안을 실현하는데서 가장 중요한 요인중의 하나로 된다. 많은 실례들에서 보게 되는바와 같이 IT보안사고들은 IT보안방책과 절차에 그들이 주의를 돌리지 않고 모르고 있는데로부터 종업원들이 범하는 부주의의 결과이다. 때문에 안전교양을 받고 숙련된 종업원들은 정보체계의 효과적인 운영과 보호에서 중요한 요인으로 될수 있다. 종업원들이 IT보안문제에 대하여 알고 있다면 그들은 사

고를 예방하고 조기적발하는 제일방어선으로 될수 있다. 또한 모든 사람들이 IT보안을 념려하여 관심을 모으면 자산과 정보를 그만큼 더 쉽게 더 효과적으로 보호하게 될수 있다.

정보의 비밀성, 무결성, 리용성을 보호하기 위해서는 모든 기관들이 망라된 모든 개별적사람들로 하여금 자기의 책임을 자각하도록 하여야 한다. 이를 위하여 IT체계를 보호하는데 필요한 방책과 절차들을 종업원들에게 잘 알려 주어야 한다. 그러므로 정보체계의 모든 말단사용자들은 IT보안의 기본문제들을 알아야 하며 일상사업에서 훌륭한 보안습관을 세울수 있어야 한다. 상급경영인으로부터 과업을 받으면 우선 보안의식화과정안의 목적을 정확하게 규정해야 한다. 일단 목적이 세워 지면 리용할수 있는 실행안을 포함하여 내용을 정해야 한다. 이 과정에 고려해야 할 기본요인들은 장애를 어떻게 극복하며 저항에 어떻게 대처하겠는가 하는것이다. 마지막단계는 성과를 평가하는것이다. 이 장에서는 IT보안의식화과정의 개발단계들에 대한 고찰에 기본을 둔다.

IT보안의식화과정의 첫째 단계는 책임경영진으로부터 공약을 받아 내는것이다.

목표설정

보안의식화과정내용을 개발하기에 앞서 목표 또는 목적을 세우는것이 급선무이다. 목적은 소박하게 《모든 종업원들은 자기들이 리행해야 할 기본보안책임을 알아야 한다.》라고 하거나 《기관에서 당하는 IT보안위험에 대하여 모든 종업원들이 의식하도록 하며 종업원들이 위험을 좌절시키고 IT체계를 보수하는데 중요한 관심을 가지도록 추동한다.》라고 하면 된다. 어떤 사람들은 아래에서 보는바와 같이 더 구체적인것을 세울 필요가 있다고 할수도 있다.

종업원들은 다음과 같은것을 알아야 한다.

- 물리적자산과 기억된 정보에 대한 위협
- 기밀(혹은 비밀)정보의 식별 및 보호방법
- 열린 망환경에 대한 위협
- 정보의 보관, 표식, 전송방법
- 저작권위반 또는 사적비밀관계법과 같은 준수해야 할 련방법들
- 의심되는 사고이건 확실한 사고이건 모든 보안사고들을 보고 받아야 할 사람
- 의무적으로 집행해야 할 기관 또는 부서의 해당 방책들
- 전자우편 혹은 인터네트방책과 절차

보안의식화과정의 목적을 세울 때 기관의 총적과업과 목적들을 반영하고 지원해야 한다는것을 명심하라. 바로 이 시점이 정보총괄책임자(CIO: Chief Information Officer) 또는 다른 책임 및 상급경영자들에게 실태보고를 해야 할 적절한(혹은 필요한) 때이다.

내 용 결 정

IT보안의식화과정은 IT체계들의 위험성과 취약성의 정도를 반영해야 하며 종업원들에게 그들이 창조, 처리, 전송 및 보관하는 정보를 보호해야 할 필요성을 상기시켜야 한다. 원래 IT보안의식화과정의 초점은 종업원들의 보안자각을 높이는것이다.

내용의 수준과 류형은 기관의 요구에 의존된다. 본질상 종업원들에게 그들이 보호해야 할것은 무엇이며 그것을 어떻게 보호하며 기관들에 IT체계보안이 얼마나 중요한가 하는것을 알려 주어야 한다.

실 현 방 도

보안의식화자료를 전수하는 방법과 방안들은 성희롱이나 기업륜리에 대한 종업원교양자료전수와 매우 류사하다. 사실은 이러하지만 전통과 결별하고 격식에서 벗어 날 때가 온것 같다. 다시 말하여 새로운것을 시도할 때가 온것 같다.

종업원들에게 사상을 알려 주며 훌륭한 콤퓨터보안습관을 장려할수 있는 적극적이고 흥미 있고 분발시키고 추동하는 방법들을 생각해 보라.

의식화과정의 성과는 여러가지 인기 있는 자료와 기교로써 많은 사람들을 쟁취하는 능력에 있다. IT보안의식화자료와 기교들의 실례를 다음에 제시한다.

- 포스터
- 충동을 주며 눈길을 끄는 구호제시
- 비데오테프
- 교실강의
- CD–ROM 또는 인트라네트접근과 같은 콤퓨터를 통한 보급
- 소책자 또는 선전물
- 추동하는 구호가 있는 펜, 연필, 열쇠줄(임의의 류형의 장신구)
- IT체계를 보호하는 내용이 있는 게시지
- 문과 게시판에 붙이는 풀종이
- 기업내의 소식지 혹은 해당 부서의 통보서에서 월 혹은 분기마다 만화 혹은 기사를 싣는것
- 특정주제의 뷸레찐(이 경우에는 보안경보)
- 보안문제와 관련한 월간전자우편통고 혹은 보안권고안의 전자우편방송
- 콤퓨터화면에 나타나는 보안구호 또는 가입전통보문
- 추동물로 식품을 나누어 주기, 례컨대 작은 뱀모양의 사탕을 담은 사탕통들을 나누어 준다. 《XYZ에 비루스가 공격개시한다》이라는 제목을 단 카드를 꾸레미에 붙이라. 《망에서 꿈틀거리는 모든 비루스를 죽이라–당신의 모든 항비루스쏘프트웨어들이 움직이도록 하라》와 같은 묘한 통보문을 주라.

Web싸이트주소 : http://awarenessmaterials.homestead.com/에서는 다음과 같은 선택항목들을 목록에 주고 있다.

- 《우리 환자의 정보를 보호하는것이 건강이다. 우리 정보를 보호하는것이 건강이다.》라는 표어를 붙인 응급치료함
- 《누가 우리 정보들을 책임지고 있는지 보라.》라는 구호를 붙인 거울
- 《당신의 통과암호는 이 치솔과 갈다 : 그것을 정기적으로 리용하며 자주 교체하라. 그리고 그것을 다른 사람과 같이 쓰지 말라》라는 구호를 붙인 치솔
- 《보안에 대하여 생각하라.》라는 구호와 교체할수 있게 된 휘장받치개
- 《당신은 훌륭한 보안열쇠이다.》라는 구호를 붙인 열쇠형식의 자석
- 《정보보호에 언제나 비쳐 주라.》라는 구호가 있는 손전지

의식화과정에서 또하나의 중요성과 요인은 의식화과정은 끝나지 않는다는것 즉 의식화깜빠니야는 기본사상을 계속 반복하여야 한다는것을 기억하는것이다. 주려는 사상이 아주 중요하다면 더 자주 반복하여야 한다. 그리고 매번 다르게 반복하여야 한다. IT보안의식화는 계속되는 운동이기때문에 모든 교양대상들의 관심이 유지되게 하자면 창조성과 열성이 요구된다. 의식화자료는 IT보안이 기관뿐아니라 모든 종업원에게 다 중요하다는 분위기를 조성해야 한다. 또한 IT보안방책과 행동준칙을 준수하는데 사람들의 흥미를 불러 일으켜야 한다.

의식화과정은 갱신되여야 한다. IT보안방책이 변경되는 경우에는 종업원들에게 통지하여야 한다. 최신정보를 전송하기 위한 기술수단을 설치하는것은 필요하며 또 유익한것이다. 실례로 다음번 《라브바그》비루스가 밤새 순환하였다면 체계경영자는 가입전통보문을 모든 워크스테이션들에 보내 주어야 한다. 기계를 시동시킬 때 사용자가 보게 되는 첫 항목은 무엇을 찾고 무엇을 열어야 하는가와 같은 체계보안정보이다.

마지막으로 보안의식화깜빠니야는 단순해야 한다. 기관들에서 의식화깜빠니야를 벌리는데 자금을 너무 많이 쓴다든가 복잡하거나 지나친 기술을 리용할 필요는 없다. 종업원들이 정보를 쉽게 접수하게 하며 또 그것을 쉽게 리해하도록 해야 한다.

보안의식화과정은 :

- 경영진이 솔선 수범으로 지원하고 이끌어야 한다.
- 단순하고 직선적이여야 한다.
- 적극적이고 주동적이여야 한다.
- 끊임 없는 사업으로 되여야 한다.
- 가장 중요한 사상을 반복해야 한다.
- 흥취가 있어야 한다.
- 적당한 경우에 유모아적이여야 하며 따라서 기억에 쉽게 남는 구호가 되여야 한다.
- 모든 종업원들에게 위험이 어떤것인가와 체계보호를 위한 임무를 알려 주어야 한다.

어떤 기관의 경우에는 의식화과정의 설계와 개발을 전문자격을 가진 업체에 외탁하

는것이 필요한(혹은 실행할수 있는) 선택안일수 있다. 기관의 요구를 들어 줄수 있는 가장 적합한 업체를 찾기 위하여 인터네트에서 제품과 봉사를 자세히 찾아 보고 다른 사람들과 만나서 그들의 경험을 들어 볼수 있다. 그리고 지난 기간의 경험을 목록화하여 가지고 있으며 제기된 목표에 대한 해결책을 개괄하여 주는 제안을 판매자에게 요구할수 있다.

장 애 극 복

전체 종업원규모의 사업에서처럼 보안의식화깜빠니야는 고위경영자의 지원을 받아야 한다. 프로그람개발을 위한 재정적지원도 받아야 한다. 례로서 매해 경영자는 의식화자료와 의식화사업자금을 할당해야 한다. 목적들, 로력 및 다른 자료에 대한 자료계산서, 시간계획서를 포함한 사업계획을 작성하라. 그리고 구체적인 가능한 문제들을 세워야 한다(즉 15분비데오, 펜, 연필 등). 경영자로 하여금 계획을 승인하고 보안의식화자료를 만들고 완성하기 위한 특별자금을 할당하도록 하여야 한다.

일부 종업원들에게 의견이 좀 있을수 있다는것을 명심하라. 이런 종업원들은 협의회에 참가하지 않고 절차를 무시하며 보안방책을 위반함으로써 부정적인 분위기를 조성하게 될것이다. 또한 종업원이 보안조치를 고의적으로 반대하면서 방책상 문제를 놓고 경영자와 싸우는 드센 반항도 있을수 있다. 실례로 여러 기관들에서는 워크스테이션의 플로피디스크구동기를 달아 놓아 망에 비루스가 침투 못하게 할수도 있다. 종업원이 매우 불손하게 나온다면 경영자는 플로피디스크구동기가 동작하지 못하게 하는것을 금지시킬수도 있다. 이렇기때문에 의식화깜빠니야와 이어 진 보안절차를 시작하기전에 경영인의 지원을 받는것이 중요하다.

일부 종업원이 반대한다 하더라도 대부분의 종업원들(필자는 이런 종업원이 98%라고 확신한다.)은 자기 일을 잘하려고 하며 정확히 하고 규정대로 하려고 한다. 부정적인 자들이 있다고 해도 주저하지 말아야 한다. 당신의 노력을 헛되게 하지 말라. 콤퓨터보안이 너무도 중요하므로 몇사람의 방해자가 있다고 해도 기관의 훌륭한 보안실행을 단념할수는 없는것이다.

회사들은 흔히 의식화과정을 찬성은 하지만 인적 및 재정적자원은 할당하지 않는다. 거기에 구애되지 말아야 한다. 계획은 크게 하고 시작은 적게 하라. 전자우편통보문을 보내거나 소식지에 통보를 싣는것과 같이 단순한것은 첫 단계에서 비용이 적게 들면서도 효과적일수 있다. 경영자들이 의식화자료의 효과를 알기 시작할 때면(물론 경영자들은 알게 될것이다.) 경영자들은 필요한 자원을 할당할수도 있다. 중요한것은 현재 있는 자원으로(혹은 자원이 없어도) 자기가 할수 있는 모든것을 계속 애 써 해나가는것이다.

종업원들은 IT체계를 보호하는데서 유일하게 가장 중요한 요인이다. 훌륭한 보안실천에 대하여 인식하면 사용자들은 정보가 안전하게 리용되게 할수 있다.

Web page주소：http://www.frentiernet.net/～mlambert/awareness/에 게재된 CISSP인 Mike Lambert의 보안의식화요령을 보라.

평　가

보안의식화과정을 비롯한 모든 경영계획을 주기적으로 검토평가해야 한다. 대부분의 기관들에서는 공식적인 량적 및 질적분석을 진행할 필요가 없을것이다. 사람들의 행동과 태도가 변하였는가 하는것을 격식이 없이 검토감시하는것으로도 충분할것이다. 아래에 고려하여야 할 몇가지 간단한 선택안들을 제기한다.

1. 종업원들에게 그들이 써넣을 조사서와 질문표를 나누어 주라. 신입사원강습기간에 의식화강습을 하였다면(정해 진 3～6개월기간이 지난후에) 강습을 다시 하여 리해정도를 알아 보라(즉 기억하고 있는것은 어떤것인가, 어떤 정보를 더 알고저 하는가 등…).
2. 아침에 커피한잔을 들면서 방에 있는 다른 사람들에게 의식화깜빠니야에 대하여 물어 보라. 그들이 새로운 포스타를 좋아 하는가, 모임을 하는 기간에 과자와 에스키모를 좋아 하는가, 콤퓨터보안에 대한 종업원들의 의식과 책임을 높이는것이 목적이라는것을 기억하라. 그리하여 지어 《그 포스타는 어리석다.》라고 응답하더라도 조급해 하지 말라. 이미 예견하였던 그대로이며 중요한것은 그것이다.
3. 의식화깜빠니야 전후에 일어 나는 보안사고들의 수와 그 류형을 장악하라. 아마도 보고되는 사고의 건수가 늘어 나면 그것은 좋을것이다. 그것은 사용자들이 콤퓨터보안위반 혹은 사고가 아닌가고 의심스러워 하는 경우에 어떻게 하며 누구에게 보고해야 하는가를 알고 있다는 표시이다.
4. 사용자의 행동을 《불시점검》하라. 사무실을 순회하면서 사용자가 없는데 워크스테이션이 망에 가입되였는가 혹은 기밀매체들(플로피디스크나 CD들)을 잘 보관하고 있는가를 검열하라.
5. 내부망을 통하여 의식화자료들을 내보내는 경우에는 강습생들의 이름과 완성상태를 기록하라. 누가 자료를 다 보았는가를 정상적으로 검열해 보아야 한다. 자료를 다 본 사람들에게는 계획된 질문서를 보낼수 있다.
6. 종업원통과암호들에 대하여 통과암호해제프로그람을 체계관리자가 실행하게 하라. 이것이 실행되면 독립콤퓨터에 프로그람을 기동시키고 망에 그것을 설치하지 않는것이 좋다. 흔히 망봉사기에 이런 류형의 쏘프트웨어를 설치할 필요는 없다. 인터네트로부터 구입할수 있는 통과암호해제무료프로그람은 흔히 악성코드를 가지고 있으므로 기다리고 있는 해커에게 통과암호목록을 보내게 되여 있어 경계해야 한다.

보안의식화과정의 본래의 목적 혹은 목표가 작성되였는가 하는것을 평가공정에서 검토하고 답변해야 한다는것을 명심하라. 때때로 잘못 선택된 항목을 집중적으로 평가한다. 실례로 의식화과정을 평가할 때 지난해에 얼마나 많은 사고들이 일어 났는가 하는것을 매 종업원에게 물어 볼 필요는 없을것이다. 그러나 보안사고가 있는것 같다고 생각할 때에는 련계를 가져야 할 사람을 아는지 매 종업원에게 물어 보는것은 좋을것이다.

요　약

종업원들은 정보체계보안계획의 유일하게 가장 중요한 요소이며 경영진의 지원은 의식화과정의 성공을 담보하는 열쇠이다.

보안의식화과정은 기관의 정보체계보안계획에서 기본으로 되여야 한다. 체계보호에 필요한 운영 및 기술적대처안외에 의식화(와 강습)는 필수적인것으로 된다. 각이한 범죄통계는 위험의 65～70%가 내부에서 일어 난다는것을 보여 준다. 이것은 기관종업원들의 60%가 체계에 대한 해커로 되고 있다는것을 의미하지는 않는다. 이것은 의식적이건 무의식적이건 종업원들이 체계에 일정한 형태의 해를 줄수 있다는것을 의미한다. 이것은 화면보호프로그람의 비법복사판적재, 인터네트로부터 공유웨어의 내리적재, 약한 통과암호의 사용, 다른 사람들과의 통과암호의 공유가 바로 그러한것들이다. 그러므로 종업원들은 IT체계의 《행동규칙》과 훌륭한 콤퓨터보안기술의 실행방법을 알아야 한다. 나아가서 련방기관들의 모든 련방공무원들은 법(1987년 콤퓨터보안관계법)에 따라 매해 보안의식화강습을 받아야 한다.

보안의식화과정은 기관의 구체적인 필요에 따라 작성되여야 한다. 첫 단계에서는 과정의 목표(무엇을 달성해야 하는가)를 결정하고 다음에는 과정계획을 세워야 한다. 이 계획은 전문가적견지에서 경영자에게 제출되여야 한다. 과정은 인원, 자금 및 도덕적지원 등의 성과를 거두는데 필요한 자원들을 보장받게 할것이다. 초기에는 리용할수 있는 자원이 부족하다 하더라도 간단하고 비용이 들지 않는 방법으로 정보를 분배하는것부터 시작하라. 시작해 놓고 더 많은 자원을 찾아 내며 다음에 주요한 IT팀성원들로부터 방조를 받는것이 중요하다는것을 명심하라.

강　습

강습은 의식화과정보다 더 공식적이며 대화적기능이 더 강하다. 사업능력과 사업능률을 높여 주는 지식을 쌓고 기술을 련마하며 능력을 키워 주는 방향에서 강습을 주어야 한다. 강의를 오랜시간 지루하게 할것이 아니라 대화적이고 내용 있는 강습을 해야 한다. 지식을 어떻게 전달하는가에는 관계없이 구체적인 지식만 가지고 있는 강사를 선발하던 시기는 이미 지나갔다. 강습(즉 양성)은 지금 전문가들이 교육리론, 절차 및 기교를 알것을 요구하는 사업이다. 강습에서는 청강자들이 강습을 마치면 자기 일에 적용할수 있는 기술과 실천기능을 높여 나갈수 있게 하는데 집중해야 한다. 강습은 또한 추동력을 줄수 있어야 한다. 따라서 강습에서는 청강자들에게 더많이 배우려는 호기심을 불러 일으켜야 한다.

지난 10년간 정보체계보안양성분야에서는 정보기술의 급속한 발전에 보조를 맞추기 위한 시도가 있었다. 한가지 실례는 표준 및 기술중앙연구소(NIST)문건 SP 800–16《IT보안강습요구사항: 역할 및 수행모형》이다. 1998년에 작성된 이 문건은 IT보안강습계획을

개발하는 련방기관들에 지도서를 제공해 준다. 사영분야의 기관인 경우에도 NISTSP 800–16이 어떤 류형과 수준의 정보를 제공해야 하는가에 대한 기준선을 규정하는데 도움이 될수 있을것이다. 이런 리유로 하여 이 장에서는 NIST문건을 간단히 고찰한다. 이 장에서는 계속하여 강습을 위한 전통적인 교수체계구성안 ISD의 단계 즉 요구분석, 목표제시, 설계, 전개, 실현, 평가를 취급한다. ISD안은 교수계획에 대한 체계적인 고찰을 제공하며 매 단계들사이의 중요한 관계와 련계를 강조한다. ISD안에서 의의 있는 기본측면은 양성목적을 내용자료의 련속적인 설계와 전개에 두는것이다. ISD안은 강습을 받고 나서 강습생이 무엇을 하며 무엇을 할수 있겠는가에 중심을 두면서 시작하게 된다. 이렇게 시작하지 않으면 나머지 단계들은 비능률적이며 비효과적인것으로 될수 있다. 그러므로 첫 단계에서는 강습의 필요성과 목표를 준다. 설계 및 전개단계에서는 내용, 교수전략 및 강습방법들이 결정된다. 실현단계는 자료의 실제적인 전수단계이다. 일반적으로 전수내용에 대한 평가가 실현단계이후에 있게 되는것으로 보지만 이런 평가는 강습의 전과정에서 계속되는것으로 보아야 한다. 지도서의 마지막부분에서는 제기된 IT보안과정안을 제공한다. 이 과정안에는 IT체계를 보호하는데 요구되는 각이한 직무의 역할을 수행하는데 필요한 여러 학과목들이 있다. 기관의 과정안은 설정된 강습의 필요성에 부합되여야 한다는것을 명심하여야 한다.

NIST SP 800–16《IT보안강습요구사항: 역할 및 수행모형》(NIST Web site http://csrc.nist gov/nistpubs/에서 구입할수 있음)

NIST SP 800–16 IT보안학습련속과정은 정보체계보안강습과정작성의 기본틀거리를 제공한다. 의식화과정을 시작한 다음 강습에로의 이행단계는《보안기초 및 인식》이다.《보안기초 및 인식》의 교수목표는 주요보안관계술어와 개념을 주어 보안지식의 토대를 쌓는것이다. 이 기초지식은 모든 기타 강습과목의 기초로 된다.

구체적인 작업명으로 종업원들을 갈라 보는 경향이 있지만 NIST SP 800-16보안학습련속과정의 목표는 정보기술과 관련된 직무명이 아니라 직무기능에 집중하는것이다. NIST의 IT보안학습련속과정은 변하는 로동력과 관련하여 마련된것이다. 즉 종업원들의 역할이 달라 지기때문에 다시 말하여 기관이 달라 지기때문에 IT보안강습에 대한 요구도 역시 달라 진다. 10년전의 체계관리자의 책임과 일상 업무를 오늘과 비교하여 생각해 보라. 그 과정에 종업원들은 IT체계와 관련하여 각이한 역할을 습득하게 될것이다. 그러므로 SP 800–16에서는 체계관리자가 해당 과정안을 요구한다고 하는것이 아니라 해당 IT체계기능을 책임진 사람이 해당 형태의 강습을 요구하게 될것이라고 지적하고 있다.

본질상 어떤 IT체계의 보안효과가 요구되는가 하는것을 결정하게 되는것은 직업기능과 해당한 책임인것이다. 이런 견해에 의하면 종업원은 여러가지 직업상 요구를 지니게 될것이며 따라서 여러가지 의무를 수행하자면 여러가지 등급의 IT보안강습을 요구하게 될것이다. 이런 새로운 견해를 인정하고 표준직무류형들을 기본구상에 맞추려고 하는것은 하나의 난점으로 될수 있다. 어떤 기관들에서는 이것이 불가능할수 있다. 그러나 직능 혹은 기관에 무관계하게 IT체계보안과정안에는 몇가지 IT보안문제들이 포함되여야 한다. 기관의 당면한 필요성에 따라 해당한 강습과정안을 선택적으로 진행하여야 한다는것을

항상 명심하여야 한다.

리상적으로는 모든 기관들이 IT보안강습과정의 모든 측면에 즉시적으로 투자할 재정적자원을 가지고 있을것이라고 볼수 있을것이다. 그러나 자원사정으로 강습을 해야 할 필요성을 따져 보지 않으면 안되는것이 현실이다. 어떤 경우에는 즉시적인 강습의 필요로부터 강습의 앞부분이나 1장만 주게 되는 경우도 있다.

경영자측의 지원

과정안내용을 분석하고 전개하기에 앞서 강습프로그람의 첫 난관의 하나로 되는것은 각급 기관들과 특히는 상급경영측으로부터 자원을 받기 어려운것이다. 어느 기관에나 강습을 주자고 하는 사람들과 일하면서 배우는것을 주장하는 사람들이 있다. 다시 말하여 어떤 경영자들은 강습이 아주 중요하며 따라서 재정적으로 지원하려고 하나 다른 경영자들은 강습에 돈을 쓸수 없으며 따라서 종업원들은 일을 하면서 필요한 기술을 배워야 한다고 한다. 그러므로 중요한 첫 단계는 회사가 보장하는 강습이 가치가 있고 필수적인것이라는것을 상급경영자들에게 인식시키는것이다.

> 상급경영자는 강습이 모든 사람들의 사업항목에서 제일 웃자리에 있다는것을 리해할 필요가 있다. 종업원들이 새로운 기술을 요구하는 일을 할것을 바란다면 강습의 가치를 잘 고려하고 평가해야 한다.

강습을 후원하는것이 중요하다는것을 상급경영자들에게 설득시키자면 다음과 같은 내용을 알아야 한다.

1. 강습은 종업원들의 사퇴를 막는데 도움을 준다. 《아니요, 그건 맞지 않소. 우리는 우리의 종업원들을 강습주는데 돈을 썼지만 그들은 떠나게 되며 결국 배운 기술을 다른 회사에로 가져 가게 되오.》이렇게 말하는 사람들은 하나는 알지만 다른것은 모르는 사람들이다. 그런 종업원들은 어쨌든 떠나 갈것이다. 그러나 전반적인 종업원들은 자기 일을 하다가 난관에 부닥치면 회사에서 기능을 높여 줄것이라고 믿는다. 그러므로 회사는 결국 행운을 만나게 될것이다.
2. 강습을 주장할수 있는 경영자들속에서 동맹자를 찾아 내야 한다. 상급경영자들이 기업계획을 토론할 때 회의에서 누구든지 강습계획에 대하여 긍정적으로 발언하도록 하는것이 중요하다.
3. 강습이 기관의 요구를 반영하도록 해야 한다. 많은 경우에 강습에서 혜택을 입게 된다는것을 경영자들에게 납득시킬 필요가 있을것이다. 이것은 실행자가 현존 계획의 약점을 알아야 하며 강습을 주면 지금까지 풀리지 않던 문제들이 풀릴수 있는가를 알려 주어야 한다는것을 의미한다.
4. 강습계획을 모든 종업원들에게 알려 주라. 일부 종업원들은 기술을 쉽게 배울수 있으므로 강습을 받으면서 시간을 보낼 필요가 없다고 생각한다. 그러므로 종업원들의 기업상 요구를 강습에서 어떻게 해결하는가를 강조하는것이 중요하다.
5. 작은 규모에서 시작하여 성과를 거두라. 초기계획이 훌륭하였다면 경영자는 강습

에 자원을 더 잘 할당할수도 있을것이다.

6. 경영자의 반대조건을 알아 내라. 상정되는 문제나 난점을 알아 내라. 강습과정안에서 그들이 좋아 하는것과 좋아 하지 않는것을 밝히라. 리용되는 강습과정안이 이런 난점들을 극복할수 있게 하라. 과정안에 경영자의 구상을 반영하라. 과정안이 모든 사람들의 희망을 다 만족시킬수는 없지만 대부분의 사람들의 요구를 만족시킬만한 가치가 있게 하라.

정보체계보안강습의 요구설정

경영자의 승인을 받은후 강습과정안개발의 첫 단계는 강습의 요구를 제기하고 그것을 규정하는것이다. 종업원이 맡은 일을 수행할수 있는 지식과 기술기능수준을 가지고 있지 못하는 경우에 강습의 요구가 제기된다. 이것은 또한 해당한 작업에 대한 사업능률표준안들이 있어야 한다는것을 의미한다. 사업능률표준안에는 작업내용과 그 수행에 필요한 지식, 기술기능, 능력 및 경험(KSA & E)이 반영되여야 한다. 그다음에는 종업원이 현재 소유하는 KSA & E와 제기된 작업을 성과적으로 수행하는데 필요한 KSA & Es을 비교하라. 이것들사이에 있게 되는 차이가 강습의 요구로 된다.

정보체계보안분야에 있는 정부의 몇개 기관들은 직능표준을 규정하였다. NIST SP 800–16외에도 전국보안통신 및 정보체계보안위원회(NSTISSC)는 정보보안(INFOSEC)강습표준규정을 제기하였다. 실례로 NSTISSC는 네가지 특정한 IT보안직능 즉 정보체계보안전문가들(NSTISSC＃4011), 지정승인기관(NSTISSC#4012), 정보체계보안의 체계담당관리자(NSTISSC#4013)와 정보체계보안관(NSTISSC#4014)을 위한 전국강습표준규정을 제기하였다. NIST와 NSTISSC문건들은 정보체계보안과제 및 책임을 수행하는데 필요한 표준규정을 확정하는데 도움이 될것이다.

일단 요구사항들을 분석한 다음의 단계는 강습의 요구사항들에 우선권별로 순차를 정하는 단계이다. 이런 단계를 결정할 때 법적요구들, 비용의 효과성, 관리의 긴박성, 기관의 취약성, 위험, 정보의 비밀성과 위험요소 그리고 강습생은 어떤 사람들로 한다는것과 같은 여러가지 요인들을 고려하여야 한다. 어떤 기관들(즉 련방기관들, 은행, 보건기관들)의 법적요구사항들은 진행하게 되는 강습내용선택을 지정하여 준다. 비용의 효과성을 알자면 강습 받지 못한 직원들에게 주는 비용에 대하여 생각하라. 실례로 망의 실패와 관련한 비용은 큰것이다. 보안체계가 닫기고 기관의 IT운영이 장기간 멎게 되면 자금손실과 시간랑비는 엄청나게 된다. 그러므로 체계관리자들에 대한 강습에 1차적인 우선권을 부여해야 한다. 그것은 행정적부하를 가장 많이 안고 있는 직업이 정보총괄책임자(CIO)나 IT정보관이기때문이다. 기관에서 위험요소평가를 했을 때에는 책임경영측이 가장 위험하다고 인정하는 내용에 대한 강습을 먼저 진행하게 할것이다. 마지막으로 문제성이 가장 크며 강습의 필요성도 가장 긴박하게 느끼는 강습생을 먼저 강습 받게 한다.

기술이 기하급수적으로 발전하므로 정보체계보안도 계속 발전된다. 기술이 변하는것만큼 체계의 취약성과 위험성도 커진다. 한걸음 더 나아가서 새로운 위험은 새로운 대응

책을 요구한다. 이 모든 요인은 IT체계전문가들의 강습을 계속 진행할것을 요구한다. IT보안강습과정안은 또한 그러한것으로서 전개되여야 하며 기술혁신과 더불어 확대되여야 한다.

요구분석, 표준규정의 제정, 강습대상의 순위규정목표와 목적의 결속에서 명심할것은 정보체계보안강습과정을 시작할 때 그 중요성에 대하여 경영자와 종업원에게 확신시키는 것이 필요하다는것이다. 모든 사업계획에서와 마찬가지로 강습과정의 성과도 기관의 전반적인 IT보안목표들을 실행할수 있는 능력에 달려 있다. 그러므로 이 보안과정의 시작에서 이 목표들은 명확히 규정해야 한다.

과정계획작성

강습의 대상이 주어 지면 강습과정계획을 세울수 있다. 과정계획에서는 강습과정을 만드는데 필요한 특정한 설비, 자료, 과업, 시간표, 인원, 재정원천을 개괄한다. 과정계획에서는 특정한 계획대상들을 위한 항목과 같은 수행해야 할 작업들의 순서와 내용들을 밝히게 된다. 강습관리자들이 범하게 되는 대부분의 일반적오유들중의 하나는 계획이 필요 없다고 생각하는것이다.

또 한가지 오유는 상급경영자로부터 과정계획승인을 받지 않는것이다. 과정계획에서 불가분리적인것의 하나는 계획이 실현되도록 하는것이다. 그러므로 다음 단계로 넘어 가기에 앞서 상급경영자와 함께 계획을 검토하라. 또한 이 단계에서 견해일치와 합의를 보는것은 다른 사람들을 그 일에 참가하게 하며 그들이 일의 한 몫을 맡고 있다고 느끼게끔 해준다. 이것은 성과의 주요한 요인이다.

교수전략(강습설계와 작성)

강습프로그람과정의 설계는 학습목적에 기초한다. 학습목적은 강습의 필요성에 귀착된다. 그러므로 교수전략(강습전수방법)은 학습목적을 실현할수 있는 가장 좋은 방법에 기초한다.

교수전략을 선택하는데서는 학습목적을 위한 가장 좋은 방법의 선택과 강습생의 수 그리고 강습자료를 효과적으로 전수할수 있는 기관의 능력에 중심을 두어야 한다. 문제해결의 열쇠는 학습목적, 강습생들과 기관을 리해하는것이다.

설계 및 작성단계에서는 내용자료를 개괄하고 강습내용의 절 혹은 파들을 구성한다. 종업원들이 알아야 할것과 그들이 직무를 수행하기 위하여 해야 할것에 기초하여 내용을 확정해야 한다. 필요성분석단계에서는 특정한 작업기능을 위한 과업과 임무를 수립할수도 있다. 내용이 과업과 관련된것이 아니라면 어떤 행동과 태도를 내용에 포함시키겠는가 하는 문제에 초점을 두어야 한다. 다시 말하여 목적에 부합되게 종업원들이 취할 태도와 목표수행에 필요한것을 내용에 포함시킨다. 기본은 행동과 태도에서 능력 있는 사람으로 되자면 무엇을 해야 하는가를 묘사하는것이다.

균형이 잡힌 정보체계보안강습과정에는 여러가지 학습방법이 있을것이다. 교수전략을 정하는데서 중요한 원칙의 하나는 될수록 간단하면서도 목적들을 달성하는 전략을 선택하는것으로 되게 하는것이다. 또하나의 요인은 교수자료자체이다. 모든 내용이 다 한 형태의 강습전략에 꼭 맞는것은 아니다. 즉 강습에서 성과를 거두자면 강습목적과 내용을 보고 강습생들이 배우는데 가장 좋은 방법이 무엇인가를 결정하여야 한다. 강습자료와 관련된 현행리론들중의 하나는 강습내용이 교육과 오락의 결합인 《교육유희》으로 되여야 한다는것이다. 청강생이 누구이며 내용이 어떤것인가를 보고 학습목적에 가장 잘 부합되는 결심을 채택하여야 한다.

방법결정에서의 몇가지 요령 :

- 청강자는 누구인가. 청강자의 규모와 위치를 고려하는것이 중요하다. 청강자가 많고 지리적으로 분산되여 있다면 기술에 기초한 해결책 즉 콤퓨터에 기초한(CD-ROM) 혹은 Web에 기초한 강습(인터네트를 통한 강습)은 더 효과적일수 있다.
- 기업의 필요성은 무엇인가. 실례로 제한된 액수의 려비만 청강생들이 리용할수 있는 경우에는 기술에 기초한 전수가 리용될수 있다. 기술에 기초한 전수는 교통비를 낮출수 있다. 그러나 기술에 기초한 강습은 흔히 더 많은 설계 및 작성비용을 필요로 한다. 그러므로 교통비용의 일부는 기술에 기초한 해결책을 개발하는데 돌려 지게 될것이다.
- 강습내용은 무엇인가. 일부 비용들은 강사가 조정하는 비데오, Web 혹은 CD-ROM을 통한 전수에 가장 잘 맞는것이다. 가장 좋은 전수방법에 대하여 많이 토론하고 있지만(그리고 모든 사람들이 자기의 의견을 가질것이지만) 강습자료를 평가하고 의견을 줄수 있는 강습전문가들의 조언을 따르는것이 좋다.
- 어떤 형태의 학습자대화가 필요한가. 강습내용이 제일 좋은 경우는 자체진도에 따르는 개별수업의 경우인가 아니면 학급별수업의 경우인가. 일부 강습자료들은 일 대 일과 학급별수업대화에 제일 적합하지만 다른 내용은 창조적이고 대화적이며 개별화된 강습에 제일 적합하다. 실례로 청강생들이 단순히 정보를 받는 경우에는 기술에 기초한 해결책이 더 적당할수 있을것이다. 청강생들이 학급에서 문제풀기를 해야 한다면 교실에서 강습 받는것이 더 좋을것이다.
- 어떤 형태의 전수 혹은 교실활동이 적용되여야 하는가. 강습내용상 강습생들이 조작체계를 설치하거나 구성하여야 하는 경우에는 실습교실이 제일 좋을것이다.
- 강습자료는 얼마나 안정되여 있는가. 내용의 안정성은 비용문제일수 있다. 내용이 자주 변하는 경우에 입게 되는 손실은 난이성, 시간 및 자금인데 이것이 계산되여야 한다. 일부 강습전략들은 다른것보다 더 쉽게, 더 적은 비용으로 수정할수 있다.
- 어떤 형태의 기술을 강습전수에 리용할수 있는가. 이것은 강습전략을 결정하는데서 결정적인 요인이다. 최근추세는 인터네트나 인트라네트를 통하여 강습을 전수하는것이다. 이 방법을 성과적으로 적용하자면 강습생들이 정보에 접근하는 기술적능력을 가져야 한다. 실례로 대역너비로 하여 전송될수 있는 다매체량(례

음성, 비데오, 동화상)이 제한될수 있는 경우에는 CD-ROM해결책이 더 효과적일 수 있다.

강습전략에 관계없이 정보제시에 리용될수 있는 몇가지 일관성 있는 요소들도 있다. 여기에는 음성, 본문, 정화상과 동화상 그림 또는 그라프, 비데오, 연시, 모의, 실례연구, 대화련습형태들이 속한다. 대부분의 강습학과들에서는 여러가지 제시방법들이 결합된다. 이로부터 모든 청강생들에게 전송하는데서 보다 큰 유연성과 강습내용을 전수하는 가장 좋은 방법선택문제를 참작할수 있다. 리용할수 있는 강습전략에 익숙되지 않는 경우에는 강습자가 조종하는 기술에 기초한 강습전수방법에 대한 구체적인 규정을 준 제19장의 부록을 참조하는것이 좋다.

어떤 형태의 강습전략이 강습의 필요성에 가장 적합한가를 결정하는 경우에 정보의 여러가지 수단을 개척하는것이 필요하다. 개별적사람들은 사업상 기업동료들과 강습전문가들에게 이전의 경험을 물어 보고 그 응답을 따져 보아야 한다. 강습전략을 결정하는것은 강습목적, 학과목내용, 전수방법, 실행항목, 기술적능력, 시간 및 자금과 같은 리용할수 있는 자원에 기초해야 한다는것을 명심하여야 한다.

가능한 과정안

제19장 부록 2에는 IT체계보안강습학과목들로서 제공될수 있는 IT보안주제들의 전반적인 목록이 포함되여 있다. 목록은 적응성 있게 되여 있다. 기술이 변함에 따라 강습형태도 변할것이라는것을 기억하여야 한다. 기관에서 고려할수 있는것은 바로 강습과목뿐이다. 또한 강습내용들은 기업소의 특별한 강습필요성에 따라 결합되고 재분류되여야 한다.

부록들에는 제목, 간단한 내용, 예견되는 청강생들, 높은 수준의 주제목록과 알맞는 기타 정보들을 비롯하여 매 학과목에 대한 보다 구체적인 정보가 있다. 부록 2에 있는 학과목들은 정보체계보안계획의 요구를 실현하는데 필요한 기술기능들에 기초한것이다. 모든 기관들에서는 우선 양성의 필요성설정을 앞세우고 진행할 강습형태를 규정하는 사업을 한다. 이런 몇가지 문제들은 제3자적인 양성회사에서 리용할수 있기때문에 기관에서 자체의 실정에 맞는 강습학과목들을 개발할 필요는 없는것이다. 그러나 기관에서 가장 효과적인 결과를 위해서는 자기 방책들과 절차들을 보강하여 강습자료들을 자체의 실정에 맞게 해야 한다. 이렇게 자체의 실정에 맞게 하는데 외부의 자원을 리용하면 기관에서 적은 비용을 들이면서 리득을 볼수 있다.

정보체계보안강습계획의 평가

강습의 효과성에 대한 평가는 정보체계보안강습계획의 중요한 요소들중의 하나이다. 그것은 강습과정의 시작단계에서부터 계속 진행되는 과정이다. 평가사업은 강습과정의 나머지 모든 단계 즉 분석단계, 설계단계, 개발단계, 실행단계에서 반드시 계획에 포함하여 진행하여야 한다. 앞에서 언급된 NIST SP 800-16문건에 의하면 강습효과성평가

에는 명백하고 호상 련관된 다음과 같은 네가지 측정항목들이 있다. 즉

1. 학습자의 주관적인 만족과 학습에 조건들이 적합한가 하는 정도
2. 주어 진 강습생이 해당 강습에서 무엇을 배웠는가
3. 해당한 강습을 받고 난 다음 강습생들의 사업상태
4. 기관의 전반적인 IT보안강습과정가운데서 다른 형태들에 비한 이 강습의 가치

평가공정에는 네가지 측정형식이 있으며 매 형식은 네가지 목적가운데서 하나와 련관된다. 평가는 다음과 같이 해야 한다.

1. 강습이후 종업원들이 자기들의 작업수행을 자체로 평가할수 있는 정보를 산출해야 한다.
2. 강습이후 개별적강습생들의 작업수행을 종업원감독이 평가할수 있는 정보를 산출해야 한다.
3. 강사들이 학습과 교수의 수준을 높이게 하는 추세자료를 산출해야 한다.
4. 투자수익통계를 산출하여 책임공무원들이 신중한 전략적립장에서 전체 로동력의 최적결과를 위하여 여러가지 IT보안의식, 보안활용능력, 강습 및 교육항목들에 제한된 자원을 할당하게 해야 한다.

최적결과를 얻자면 자료의 수집 및 리용계획을 세우며 정보(자료)를 평가하고 그것을 기관의 목적에 따라 추정해 내기 위하여 분석가들에게 요구되는 시간에 대한 계획을 세우는것이 필요하다.

효과적인 측정 및 평가의 가장 중요한 요소들중의 하나는 알맞는 측정항목을 선택하는것이다. 그러므로 평가의 형태에 관계없이 혹은 평가가 있는 경우에는 인식력, 지식 혹은 구체적인 기술기능항목과 같은 평가해야 할것에 대하여 기관에서 합의보아야 한다.

> 로동시간 및 돈과 같은 자원들이 절실하게 요구되기때문에 강습과정의 평가는 강습계획의 전일적인 한 부분으로 되여야 한다.

평가하는데는 비용이 든다는것을 명심하라. 비용에는 생각, 시간, 노력과 돈이 포함된다. 그러므로 평가는 강습과정의 계속 진행되는 전일적인 한 측면으로 간주되여야 하며 시간과 돈은 다 예산에 잘 계획되여야 한다.

요 약

IT체계보안은 기관운영의 모든 측면과 련관되는 빨리 전개되며 위험도가 높은 분야이다. 회사들과 전반기관들은 종업원들이 자기 책임을 잘 수행하게 하며 IT체계자산과 정보를 보호할수 있게 하는 훌륭한 의식화, 강습과 교육을 종업원들에게 보장해야 할 어려운 문제를 안고 있다.

> 종업원들은 기관의 가장 기본적인 구성요소이며 강습 받은 종업원들은 정보체계를 효과적으로 실행하며 보호하는데서 결정적역할을 한다.

이 장에서는 정보체계(IS)보안양성프로그람의 각이한 측면들을 개괄하였다. 첫 단계는 의식화과정을 작성하는것이다. 의식화과정은 종업원들에게 IT보안문제들에 각성을 높이도록 하는 단계를 설정하도록 한다. 의식화과정은 또한 IT체계사용자들을 보안양성프로그람의 첫 단계에 준비시킨다. 다시 말하여 모든 종업원들에게 IT보안의 기본개념을 인식시킨다. 강습초보로부터 시작하여 각이한 특정된 구체적인 학과목들을 종업원들에게 인식시킨다. 이런 특정한 강습과목들은 기관이 IT체계보안부문에서 있게 되는 각이한 작업기능과 련관되여야 한다.

강습과정의 성과에 결정적영향을 주는것은 상급경영진의 지원과 승인을 받는것이다. 과정생명주기의 매 단계에서 중요한것은 모든 강습조성원들과 집행리사들에게 실태보고를 배포하여 그들이 발전하는 추세에 따라 가도록 하는것이다. 어떤 경우에는 다음 단계로 이행하기전에 상급경영자로부터 승인을 직접 받는것이 중요할수(혹은 필요할수) 있다.

강습진행의 다섯가지 단계들은 모든 IS보안강습과정과 련관된다. 첫 단계에서는 강습의 필요성을 분석하고 강습과정의 목표와 목적들을 세운다. 필요성이 일단 설정되면 다음 단계에서는 강습의 설계를 시작한다. 강습과정을 설계문건이나 프로그람설계도형태로 문건화하는것이 중요하다. 설계문건이 강습과정개발의 방향을 규정하기때문에 모든 당사자들은 설계문건을 집행하기에 앞서 재검토하고 승인하여야 한다.

개발단계에서는 강사자료, 강습생자료, 교실활동 등과 같은 모든 강습요소들을 묶어주게 되며 기술적인것이라면 매체요소들의 문서 및 화상만들기와 프로그람작성을 묶어주게 된다. 강습과정개발이 완성된 경우에 실현단계의 첫 목표는 자료의 시험으로 시작된다. 이런 상태에서 강습설계집단은 학습자의 효과를 위한 자료를 평가하게 되며 프로그람의 실행에 앞서 임의의 문제점을 개정하게 된다. IS보안강습과정전반에 평가과정을 포함시키는것은 그 과정의 성과를 보장하는데 전반적인 의의를 가진다. 시간이나 돈과 같은 자산은 강습자료의 효과성을 평가하는데 그리고 학습과 회사의 필요성을 만족시키는데 리용하여야 한다. 평가과정의 기본요인은 IT보안강습과정의 설계, 개발 및 실현단계

에 평가과정을 포함시키는것이다.

강습학과목의 몇가지 견본들이 IS보안강습과정에 건의되였다. 기술이 변함에 따라 커지는 IT보안의 난관들을 극복하는데 필요한 강의과목들도 변하여야 한다. 이런 변화들로 하여 현재의 학과목들을 수정개선하지 않으면 안된다. 또한 부단히 변화되는 IT체계의 발전과 개선을 위해서는 새로운 학과목들을 내와야 할것이다. 그러므로 IS보안강습과정과 학과목들은 새로운 요구를 실현할수 있도록 신축성 있게 설정되여야 한다.

매 기관에서는 또한 IT전문가들의 장성계획을 세워야 한다. IT보안기능은 기술 및 경영에서 복잡하게 되였다. 회사들은 IT보안에서 제기되는 어려운 문제들을 해결할수 있고 변화발전하는 기술문제들에 보조를 맞추어 나갈수 있는 교육 받은 IT보안전문가들을 요구하고 있다. 기관들에서는 적당한 사람들을 IT보안전문가로 선발지명하고 그들을 제기되는 문제들을 풀수 있고 선견지명이 있는 IT보안전문가들로 키워야 할것이다.

정보체계보안양성과정을 개발하는 어려운 문제에 직면하게 되는 경우 그 과정이 개별적인 한 사람에 의하여 수행될수 없다는것을 명심하는것이 중요하다. 개발계획들에 모든 부서들이 힘을 집중하도록 경영진이 조직사업을 하는것을 포함한 기관전반적인 광범한 노력과 협조가 있어야 이 보안문제를 해결할수 있다. 모든 사람들을 이 과정에 망라시키게 되면 그들에게 주인다운 태도와 책임성을 북돋아 주는 추가적인 우점이 있게 된다. 또한 일군양성(즉 경영자, 강습설계자와 강습일군양성)과 IT보안전문가양성에 대한 전문지식은 강습목적을 달성하는데 필요한것이다.

항상 최종결과를 기억하라.《훌륭한 IT강습과정은 IT체계자산과 그 정보의 무결성, 리용성, 비밀성 즉 IT보안의 최우선적목표를 담보할수 있게 한다.》

제１９장. 보안의식의 계발: 부록

쑤존 디 핸취

부록 1: 강습전략(강습전수방법)

강사지도식강습

전통적인 강습전략은 강사의 지도밑에 강습생들이 그룹별로 모여서 강습 받는 전략이다. 강습생들은 한 교실에 모이고 강사 혹은 부강사가 강습을 진행한다. 강사와 강습생들사이에는 짧은 대화가 있을수 있다. 보통 이런 강습은 강습자의 설계와 개발단계까지는 비용이 가장 적게 들지만 실행단계에서 특히 강습생들이 중심지까지 통근하여 모이게 되는 경우에는 비용이 제일 많이 들수 있다.

교재를 리용하는 강습

교재에 기초하는 강습은 개별적사람들이 자기 진도에 맞추어 학습하게 되는 강습형태이다. 강습생은 강습내용이 담긴 지정된 교재(혹은 임의의 책)를 학습한다. 교재에 기초한 강습에서는 강사와의 대화가 리용되지 못한다. 그러나 교재에 담겨 있는 정보는 보통 학습문제에 대한 전문지식이 있는 필자가 쓴것이다. 또한 강습생은 자료가 필요할 때에는 그것을 찾아서 필요한 부분들을 다시 고찰할수 있다(혹은 다시 읽을수 있다.).

해답서 혹은 과제서를 리용하는 강습

해답서 혹은 과제서에 의한 강습은 개별적인 사람들이 자기 진도에 맞추어 진행하는 강습이다. 이것은 가장 오래된 원격학습형태이다(즉 통신학습형태). 과제서에는 강습교재, 도해와 련습문제들이 있다. 련습문제들은 강습생들에게 배운 내용을 가지고 련습할수 있는 기회를 주어 과제서에 있는 내용들을 학습할수 있게 도와 준다. 일부 경우에 강습생들은 해당 주제에 대한 인식능력을 보여 주는 시험을 끝내야 한다.

비데오를 리용하는 강습

비데오를 리용하는 강습은 흔히 개별적인 사람들이 자기 진도에 맞추어 진행하는 강습형태이다. 정보는 표준VHS비데오카세트록화기(VCR)에서 쓸수 있는 표준VHS비데오카세트테프에서 받게 된다. 개별적사람들의 진도에 따라 진행하는 강습에서는 강사와의 담화가 적용되지 못한다. 그러나 교실에서 비데오를 리용하는 수업인

경우에는 비데오에서 취급되는 자료를 놓고 대화를 동반하는 련습으로 토론분석할 수도 있다.

비데오에서는 공정들 또는 단계별 항목들의 동작들을 보여 줄수 있는 움직이는 그림들을 리용할수 있다. 비데오는 전수시간과 장소에 구애되지 않으며 필요한 경우에는 학습한것을 반복할수 있다.

CBT와 WBT 등 기술에 기초한 강습

기술에 기초한 강습도 개별적사람들이 자기 진도에 따라 진행하는 강습이다. 어떤 강습에서든지 강습전습에 콤퓨터를 리용하는것이 기본으로 되고 있다. 기술에 기초한 강습인 경우에는 강습과정대로 학습할수 있게 하는 콤퓨터와 쏘프트웨어를 리용하여 강습내용을 전달한다.

이런 강습은 자기원판디스크와 CD–ROM을 통하여 전수되는 혹은 봉사기에 적재되는 콤퓨터에 기초한 강습이거나 인터네트나 인트라네트를 통하여 전수되는 Web에 기초한 강습일수 있다.

콤퓨터에 기초한 강습(CBT)에는 개별사용지도서, 실천련습문제, 모의 또는 모방, 연시련습문제와 유희를 포함하여 여러가지 전시방법들이 있다. CBT에는 많은 긍정적인 특성들이 있다. 이것들은 지리적으로 널려 있는 많은 강습생들에게 강습자료 한조를 보내 주어야 하는 기관들에서 중요할수 있다. CBT의 우점에는 즉시적인 반응, 강습자료학습에 대한 강습생들의 조종과 비데오, 음성, 소리와 동화상과 같은 다매체의 결합이 속한다.

초기 CBT개발원가가 계산되면 임의의 시간에 임의의 수의 강습생들에게 CBT를 제공할수 있다. 주문에 의하여 만든 CBT프로그람에서는 강습생들에게 필요한 문제에 중점을 둘수 있으므로 강습시간과 비용이 많이 줄어 들수 있다. CBT는 또한 강습생들의 통근비용을 줄이거나 없앨수 있다. 그러므로 총적인 강습비용은 줄어 들수 있다. 자체의 진도에 따라 진행되는 개별화된 강습형태로서의 CBT는 강습생들의 실정에 맞게 적용될수 있는 적응성을 가진다. 실제로 강습생들은 구체적인 과목이나 주제를 선택하여 강습환경을 조종할수 있다. 비록 CBT가 많은 우점을 가지고 있지만 그것이 강습의 모든 필요성을 다 만족시키지는 못한다는것을 기억하는것이 중요하다. 일정한 조건에서는 CBT가 더 적당하고 효과적이며 비용도 덜 든다. 그러나 다른 경우들에는 강습생들의 부정적인 태도를 발로시킬수도 있고 강습과정의 목표를 망치게 할수도 있다. 실례로 CBT강습을 받게 된 강습생들은 강습시간표를 짤데 대한 지시를 받고 강습을 근무시간외에 받게 될것이라고 생각한다. 이들은 강사의 지도를 받으면서 강습 받는 강습생들이 근무시간내에 학습한다고 생각하므로 CBT에서는 공정하지 못하게 시간을 요구한다고 볼수도 있다.

CBT에는 교실에서 진행하는 강습과 같은 전통적인 학습환경에서 도움을 주는 도구로서 콤퓨터를 사용하는 콤퓨터지원학습(CAL)도 포함된다. 콤퓨터는 강습공정에서 투영기나 인쇄물과 같이 강습자에게 도움을 주는 장치이다. CBT는 콤퓨터에서 개별적사람들의 성적을 평가하는 콤퓨터지원시험(CAT)도 포함한다. 강습생들은 콤퓨터상에서 시험을

치고 콤퓨터는 시험을 기록하고 성적을 종합한다. CAT는 대부분의 콤퓨터에 기초한 강습제품에 포함되여 있다.

Web에 기초한 강습(WBT)은 널리 퍼져 있는 무제한한 청강생들에게 콤퓨터에 기초한 강습을 전수하는 새로운 창조적인 방법이다. WBT는 CBT의 현재 전수에서 갈라 져 나온것이다. CBT형식에서는 정보를 국부장치, 봉사기 또는 CD–ROM에 보관한다. WBT에서는 정보가 Web을 통하여 분포되며 대체로 먼곳 혹은 기관의 중심봉사기에 보관된다. 정보는 인터네트탐색기와 같은 열람기라고 불리우는 쏘프트웨어응용프로그람을 통하여 사용자에게 연시된다. 내용은 본문, 도해, 음성, 비데오와 동화상에 의하여 제시된다. WBT는 시간절약과 용이한 접근들을 비롯하여 CBT와 동일한 많은 우점들을 가진다. 그러나 CBT에 비한 WBT의 중요한 우월성의 하나는 정보를 쉽게 갱신하는것이다. 강습자료를 바꾸어야 할 필요가 제기되면 봉사기에서 정보를 바꾼다. 그렇게 되면 누구나 새로운 정보에 접근할수 있다. WBT의 난관은 강습생의 콤퓨터, 기관의 봉사기와 리용할수 있는 대역너비에 기술적능력을 보장하는것이다.

부록 2: IT체계보안강습과정안

INFOSEC 101 IT 보안기초

개괄 이 과정안에는 IT체계의 모든 사용자들이 알아야 할 중요술어와 개념들, IT보안의 근본문제들과 그것들을 적용하는 방법 그리고 IT체계보안행동규칙들이 서술되여야 한다. 이렇게 되면 IT체계재부와 정보를 보호하는데서 모든 개별적사람들이 자기들의 역할이 어떠해야 한다는것을 알게 될것이다.

강습대상 이 강습은 특정한 직무에 무관계하며 IT체계를 사용하는 모든 종업원들을 위한것이다. 한마디로 말하여 모든 종업원들이 이 강습을 받아야 한다.

강습내용 IT보안은 무엇이며 왜 그것이 중요한가 ; 련방법률 및 규정들 ; IT체계의 취약성, 위험 및 예민성 ; 민감하지만 비밀화되지 않은 정보와 비밀화된 정보를 포함한 정보의 보호 ; 하드웨어보호, 통과암호보호 ; 매체취급(즉 플로피에서 정보의 처리, 보관 및 없애는 방법) ; 저작권 문제 ; 무료형콤퓨터보안 ; 사용자책임 ; 문제가 생길 때 련계 가질 사람 ; 모든 IT체계사용자들과 련관된 다른 특정한 기관들, 기관이 비밀화된 정보를 처리하는 경우에는 그것과 관련한 해설을 주어야 한다는것을 알아 두라.

주의 대부분의 기관들이 모든 종업원들에게 이 강습을 주려고 하기때문에 이 강습비용은 기술설비들을 통하여 전수되는 강습내용의 좋은 본보기로 된다. 이 강습에서는 비데오를 리용하는 강습, CD–ROM을 통하여 콤퓨터를 리용하는 강습 혹은 기관인트라네트를 통하여 Web만을 리용하는 강습형태들을 리용하게 된다.

표 19-1 제기된 정보체계보안강습과정안

과정안번호와 내용수준	과정안명칭	강습대상	가능한 전제과목
INFOSEC 101 초급	IT보안기초	모든 종업원	없음
INFOSEC 102 초급	비밀정보를 처리하는 망IT보안기초	비밀정보를 처리하는 망에 접근하는 모든 종업원	없음
INFOSEC 103 초급	IT보안기초―년례재교육	모든 종업원	INFOSEC 101
INFOSEC 104 초급	IT보안기본원리	IT보안을 직접 책임진 사람들	없음
INFOSEC 201 중급	IT체계보안계획과 개발	IT체계보안계획의 개발을 책임진 사람들	INFOSEC 101 또는 103
INFOSEC 202 중급	IT체계사고방지계획의 개발방법	IT체계사고방지의 계획의 개발을 책임진 사람들	INFOSEC 101 또는 103
INFOSEC 203 중급	IT체계보호를 위한 체계 또는 기술적책임	IT체계의 계획 및 일상 조작을 책임진 사람들	INFOSEC 101 또는 103
INFOSEC 204 중급	IT체계보안을 위한 생명주기계획화	IT체계의 리해와 설계를 책임진 사람들	INFOSEC 101 또는 103
INFOSEC 205 중급	기본정보체계보안관 (ISSO)강습	ISSO 또는 대리 ISSO로 임명된 사람들	INFOSEC 101 또는 103
INFOSEC 206 중급	IT체계의 검증	임명된 검열관역할을 담당한 사람들	INFOSEC 101 또는 103 INFOSEC 203
INFOSEC 207 중급	책임경영자들을 위한 정보체계보안	책임리사수준의 경영자들	없음
INFOSEC 208 중급	망 및 인터네트보안개론	망접속을 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 203
INFOSEC 209 중급	암호학개론	망접속 정보 및 보안을 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 203 또는 205
INFOSEC 301 상급	검열기록부 료해	검열기록부재검토를 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 203 또는 205
INFOSEC 302 상급	Windows NT 4.01보안	Windows NT 4.01을 사용하는 망을 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 203
INFOSEC 303 상급	Windows 2000보안	Windows 2000을 사용하는 망을 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 203
INFOSEC 304 상급	UNIX보안	UNIX를 사용하는 망을 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 203
INFOSEC 305 상급	상급ISSO강습	ISSO 또는 대리 ISSO로 임명된 사람들	INFOSEC 205
INFOSEC 306 상급	사고처리	IT보안사고처리를 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 205
INFOSEC 307 상급	위험분석 및 평가를 진행하는 방법	위험분석을 책임진 사람들	INFOSEC 101 또는 103 INFOSEC 205

비밀정보를 처리하는 망을 위한 INFOSEC 102 IT보안기초

개괄 이 강습은 IT체계의 모든 사용자들이 알아야 할 주요술어와 개념들, IT보안의 근본원리들과 그것을 적용하는 방법 및 행동규칙들을 해설한다. 이 강습은 비밀정보를 처리하는 망에 접근하는 종업원들에게 적합한 정보를 주기도 한다는것이 다를뿐 INFOSEC 101과 류사하다.

강습대상 이 강습은 비밀정보를 가공하는 망에 접근하는 모든 종업원들을 위한것이다.

강습내용 IT보안이란 어떤것인가 그리고 그것이 왜 필요한가；련방법률과 규정들；IT체계의 취약성, 위험 및 기밀도；비밀정보의 보호；TEMPEST설비를 비롯한 하드웨어보호, 통과암호보호；매체처리(즉 비밀정보의 처리, 보관 및 삭제방법)；저작권문제；무릎형콤퓨터보안, 사용자책임；문제가 제기될 때 련계가질 사람；그리고 분류된 IT체계의 사용자들과 련관된 다른 특정한 기관방책들

INFOSEC 103 IT보안기초–년례재교육

개괄 이 강습은 IT보안기초(INFOSEC)에 이어 지는 련속과정이다. 기술이 변함에 따라 IT보안에 대한 요구와 도전도 또한 변한다. 이 과정에 기관들은 말단사용자가 당하는 가장 심각한 난관을 주시하게 될것이다. 재교육과정안의 초점은 이런 필요성을 해결하는 방법에 돌려 질것이다.

강습대상 재교육에는 IT체계를 리용하는 모든 종업원들이 참가하게 된다.

강습내용 주제들은 기관이 직면하는 련관된 IT보안의 난관들에 해당한것이다.

INFOSEC 104 IT보안의 근본원리

개괄 이 과정안은 IT체계의 보호와 직접 관련된 종업원들을 위한것이다. 이 과정안은 련방법률과 기관의 특정한 방책과 절차들, IT체계의 취약성과 위험, 그 위험을 완화시킬수 있게 하는 대응책들 그리고 물리적, 인적, 행정적 및 체계 또는 기술적조종들에 대한 근본적리해를 보장한다.

강습대상 이 과정안은 IT보안기초보다 더 많은것을 필요로 하는 종업원들을 위한것이다. 이 과정안은 더 높은 수준의 자료를 학습하는데서 필수과목으로 리용될수 있다. 이 과정안은 체계관리자, 체계운영진, 정보관, 정보체계보안관, 보안관과 프로그람관리자들을 포함한다.

주의 이 과정안은 INFOSEC 101과정안대신에 사용할수 있다. 이 과정안은 IT체계의 보안과 직접적으로 련관된 작업을 책임진 종업원들을 위한 준비과정안이다.

INFOSEC 201 IT체계보안계획의 개발

개괄 모든 IT련방체계는 법률에 따라 그 일반지원체계들과 주요응용프로그람을 위한 IT체계보안계획을 가져야 한다. 이 과정안은 NIST SP 800–18 정보기술체계를 위한 보안

계획개발지도서에 제시된 지침에 따라 어떻게 IT체계보안계획을 개발하겠는가에 대하여 설명을 준다.

강습대상 IT체계보안계획을 준비하고 실현하도록 하는 책임을 진 체계소유자(혹은 집단). 많은 기관들에서 IT체계보안계획은 체계관리자, 정보관, 보안관 및 정보체계보안관과 같은 집단에 의하여 개발될것이다.

강습내용 체계식별, 보안책임관계할당；체계설명 및 목적；체계호상련결, 정보의 기밀성과 공유；위험평가 및 관리；행정적, 물리적, 인적, 체계적 및 기술적통제방법；생명주기계획；보안의식화 및 양성

주의 이 과정안의 설계는 기관에서 승인 받은 방법과 사전에 규정한 형식으로 IT체계보안계획의 개발에 관한것으로 주문작성되여야 한다. 강습생들은 기관이 승인한 계획개발에 필요한 도구를 소유하고 강습을 졸업해야 한다.

INFOSEC 202 IT체계사고방지계획개발방법

개괄 IT체계들이 직면하고 있는 위험요소들은 기업을 계속 운영하기 위한 효과적인 계획과 재해복구계획을 잘 세울것을 요구한다. 기업을 계속 운영하기 위한 계획에는 와해상태로부터의 회복문제 및 위험기능에 대한 지원을 계속할데 관한 문제가 반영된다. 재해복구계획에는 재해로부터의 회복문제, 주요기능을 정상운영에로 복구하는 문제가 반영된다. 첫 단계는 기관의 주요 기능과 공정들을 밝히고 회복기간들과 그 대안들을 결정하는것이다. 이 과정안에서는 회복의 우선권, 호상의존처리와 회복을 요하는 기초기술하부구조를 밝히는 면밀한 기업영향분석(BIA)(기관안에서 주요기업기능들을 식별하고 최대중지가능시간이상으로 기능중지의 영향을 결정하는)을 진행하는 방법에 대하여 론의되고 있다.

강습대상 IT체계의 계획과 관리를 책임진 종업원들. 여기에는 체계행정경영자, 정보관, 보안관 및 정보체계보안관이 속한다.

강습내용 IT체계사고방지계획이란 어떤것인가, 기업영향분석(BIA)；싸이트설정(만가동싸이트, 동면싸이트, 작업싸이트)；회복목적들；회복요구사항들；회복실현；예비안과 계획；계획시험；회복시험결과의 평가

주의: 이 과정안의 내용은 IT체계사고방지계획을 작성하기 위한 기관에서 승인된 방법론을 가지고 주문하여 편성하여야 한다. 가능하면 사전에 승인된 형식과 방법에 의거하여 해야 한다.

INFOSEC 203 IT체계보호를 위한 체계적 및 기술적책임관계

개괄 이 과정안은 IT체계의 취약성과 물리적재산과 정보보호에 필요한것을 설명하는것으로부터 시작된다. 이 과정안에서는 물리적환경보호, 쏘프트웨어의 설치, 접근조종, 조작체계와 보안요구를 실현하는 응용프로그람과 같은 특정한 요구들에 초점을 둔다.

강습대상 IT체계의 계획과 일상조작에 망라되며 책임지는 종업원들.

여기에는 체계행정경영자들, 체계성원들, 정보관들 및 정보체계보안관들이 속한다.

강습내용 IT체계보안개괄 ; IT체계의 취약성, 위험 및 기밀도의 식별 ; 효과적인 대응책식별 ; 행정적임무들(즉 기록부와 기록의 관리) ; 물리적임무들(즉 봉사기실보안) ; 호상련결보안 ; 접근조종(식별과 인증) ; 작업조의 파일관리(작업조와 공유파일의 설정) ; 작업조와 파일승인(접근승인체계구성) ; 검사사건과 기록부 ; 그리고 IT보안유지

INFOSEC 204 IT체계보안을 위한 생명주기계획

개괄 체계생명주기는 시작부터 마지막까지 IT체계를 구축조작하기 위한 모형이다. 이 과정안에서는 IT체계들을 실현하기에 앞서 그 취약성과 위험식별방법의 근본원리들과 IT체계설계기간의 IT보안문제를 취급한다. 또한 IT체계의 실현단계에서 나타날수 있는 위험요소들의 식별, 이 위험요소들의 축감, 보안에 초점을 두면서 표준조작절차에 대한 해설, IT체계의 안전성시험방법, 기한완료된 자산의 처리문제들을 취급한다.

강습대상 IT체계의 리해와 설계임무를 맡은 경영자들. 여기에는 계약책임자들, 정보관, 체계관리자들, 프로그람관리자들 및 정보체계보안관이 속한다.

강습내용 설계공정에서 IT보안의 필요성확인 ; 인식단계에서 IT보안개발 ; 련방법률과 규정들 ; 기관방책과 절차 ; 인식, 개발, 설치 및 시행조종 ; 위험성관리 ; 표준조작절차설정 ; 설비와 매체의 파괴 및 처리

주의 초점은 IT보안과 련관된 결정채택활동을 위한 기관의 구조 및 공정들의 실행과 리행에 두어야 한다. 기관의 특정한 방책, 지침, 요구, 역할, 책임 및 자원할당을 사전에 설정해야 한다.

INFOSEC 205 정보체계보안관(ISSO)기초강습

개괄 여기서는 ISSO역할과 임무에 대하여 간단하게 소개한다. ISSO는 IT체계보안계획을 실현하며 IT체계에 대한 보안감시를 보장한다. 또한 IT보안의 중요성과 일상조작에서 보안관리역할을 어떻게 보장하는가 하는데 대한 리해에 기본을 둔다.

강습대상 ISSO 혹은 이와 대등한 직무에 임명된 종업원들. 여기에는 체계관리자, 정보관, 프로그람관리자 혹은 보안관들이 속한다.

강습내용 IT보안개관, 취약성, 위험 및 기밀도 ; 효과적인 대응책 ; 행정적조종, 물리적조종, 체계적 혹은 기술적조종 ; 사고처리 ; 보안의식화

주의 모든 기관들에서는 IT체계에 대한 보안감시를 책임진 정보체계보안관으로 한사람을 임명해야 한다.

INFOSEC 206 IT체계의 승인 및 보증

개괄 여기서는 IT체계가 정보보안요구에 응한다는것을 증명하는 방법에 대한 정보를 제공한다. 이 정보에는 IT체계를 특별하게 안전한 방법으로 조작하며 비밀화된 혹은 민감하지만 비밀화되지 않은(SBU) 정보를 련방 혹은 기관의 요구에 따라 보호하도록 최종승인을 주는 문제가 포괄된다.

강습대상 지적된 비준공무원의 역할과 책임을 맡은 사람들. 여기에는 프로그람관리자, 보안관, 정보관, 정보체계보안관들이 속한다.

강습내용 련방법률과 규정；기관방책과 절차；취약성, 위험 및 기밀도；효과적인 대응조치；접근조종；그룹 및 파일허가：비밀정보와 SBU정보의 보호；TEMPEST 및 다른 설비의 보호；승인과정；사건처리；생명주기관리；표준조작절차；위험관리

INFOSEC 207집행경영인들이 알아야 할 정보체계보안

개괄 이 과정안에서는 집행경영자들이 알아야 할 정보체계보안문제들에 대한 개괄을 준다. IT체계의 계획 및 관리보안의 필요성과 인적 및 재정적지원의 할당, IT보안성원들을 솔선수범으로 이끌어 주는 문제가 강조된다.

강습대상 예견되는 집행리사급경영자들

강습내용 IT체계보안개관；련방법률 및 규정；IT체계의 취약성과 위험；효과적인 대응책；IT보안관리 및 감시의 필요성；IT보안예산

주의 이 과정안의 내용은 매 기관에서 강습내용이 집행리사급의 경영진의 특정한 요구를 만족시킬수 있도록 주문구성하여야 한다. 내용이 특별한 주제들에 기초하여 몇개의 짧은 대화형의 과들로 구성할것이 예견된다. 제한된 시간을 효과적으로 리용하기 위하여 일부 과들은 기술에 기초한 응용프로그람을 통하여 전수될수 있다.

INFOSEC 208망과 인터네트보안개론

개괄 이 과정안에서는 기관의 IT체계자원과 정보를 보호하기 위한 망과 인터네트 혹은 인트라네트보안방책을 어떻게 개발하는가 하는 문제에 중심을 둔다. IT체계의 취약성분석, 각이한 외부위험재검토, 위험관리, 승인 없는 접근으로부터 IT체계의 보호, 방화벽 및 자료암호화장치와 같은 기술적대책을 전개하여 위험요소들을 줄이는 문제에 초점을 둔다.

강습대상 내부인트라네트와 외부인터네트접속을 비롯하여 망접속실현, 일상관리, 감시임무를 지닌 종업원들. 여기에는 체계관리자, 체계담당일군들, 정보관, 정보체계보안관, 보안관 및 프로그람관리자가 속한다.

강습내용 IT망보안 및 인터네트개관, TCP/IP와 파케트개론, 망접속의 취약성과 위험(해커, 위법부호, 위장, 엿보기, 봉사거절공격)리해, 망접속을 위한 효과적인 대응책들(방책들, 접근조정, 물리적보호, 항비루스, 쏘프트웨어, 방화벽, 자료암호화 등)；망 및 인터네트 혹은 인트라네트보안방책개발 그리고 인터네트공격인식법

INFOSEC 209암호학개론

개괄 이 과정안에서는 암호작용을 개괄하게 된다. 여기서는 암호학의 기초개념들, 이것들의 응용 및 적용으로서의 공통 및 전용의 주요알고리듬, 암호열쇠분배와 관리, 전자거래의 신뢰성을 보장하기 위하여 수자식서명의 리용, 부인방지가 취급된다.

강습대상 망접속들의 관리 및 보안임무를 진 종업원들. 여기에는 체계관리자, 체계담당일군, 정보관, 정보체계보안관, 보안관들 그리고 프로그람관리자들이 속한다.

강습내용 암호학개념들, 암호학적모듈을 리용하는 인증방법들 ; 암호화, 보증기관개관 ; 수자식서명 ; 부인방지 ; 하쉬함수와 통보문개요 ; 비밀열쇠와 공개열쇠암호화 그리고 열쇠관리

INFOSEC 301검사기록부의 리해

개괄 이 과정안은 검사기록부의 리해와 재검토에 중심을 두는 대화수법이다. 여기서는 어떤 형태의 사건들이 검사기록부에 등록되는가, 흔히 이상한 사건들의 탐색방법, 검사기록도구의 리용법, 검사기록부에 기록보관하는 방법, 검사에서 색출하는 흔치 않은 사건취급법을 배우게 된다.

강습대상 일상 IT체계조작의 감시관리 및 보장임무를 맡은 종업원들. 여기에는 체계관리자, 정보관, 정보체계보안관이 속한다.

강습내용 IT체계사건의 리해 ; 검사기록부재검토의 계획화 ; 검사기록재검토법, 검사기록부를 통한 발견 및 탐색법 ; 검사기록부재검토에서 제3자도구리용법 ; 검사기록부에 있는 비정상체계사건의 처리법

INFOSEC 302Windows NT 4.0봉사기 및 워크스테이션보안

개괄 이 과정안에서는 봉사기 및 워크스테이션조작체계들을 위하여 Windows NT 4.0 보안특징들을 잘 구성하는 방법에 힘을 넣는다. 청강생들은 윈도우즈 NT의 보안특징들을 배우며 실지체험을 목적으로 하는 콤퓨터학습실에 조작체계들을 설치구성하는데 참가한다.

강습대상 이 과정안은 Windows NT 4.0봉사기 및 워크스테이션조작체계를 리용하여 망을 설치, 구성, 관리하는 임무를 맡은 종업원들을 위한 과정안이다. 정보관, 체계관리자들, 체계담당일군들이 이 과정안을 배울수 있다.

강습내용 Windows NT 4.0봉사기와 워크스테이션조작체계 개관 ; 식별 및 인증조종 ; 임의의 접근조종 ; 그룹구성 및 허가 ; 체계파일의 보호 ; 사건검열 ; Windows NT도구들의 리용 ; 체계의 구성 및 유지

주의 강습생들이 INFOSEC 203을 완전히 학습하여 IT보안개념에 대한 기본적인 리해를 가지는것이 필수적인 전제로 된다.

INFOSEC 303 Windows 2000보안

개괄 이 과정안은 Windows 2000조작체계의 보안특성들을 잘 구성하는 방법에 기본을 둔다는것외에는 INFOSEC 302와 류사하다. 강습생들은 실체험적인 콤퓨터학습실에 조작체계를 설치구성하면서 Windows 2000의 보안특성들을 배운다.

강습대상 이 과정안은 Windows 2000조작체계를 리용하는 망들의 설치, 구성 및 관리

를 책임진 종업원들을 위한 과정안이다. 이들가운데는 정보관들, 체계관리자들과 체계담당일군들이 있게 된다.

강습내용 Windows 2000조작체계개념 ; 령역이름체계(DNS) ; 이동하는 Windows NT 4.0령역들 ; 식별 및 인증조종 ; 임의의 접근조종 ; 파일체계자원(NTFS) ; 그룹구성과 허가 ; 등록부 및 파일조직과 허가 ; 체계파일보호 ; 사건검사 ; Windows 2000도구를 리용한 체계의 구성 및 유지

주의 강습생들이 INFOSEC 203을 완전히 학습하여 IT보안개념들에 대한 본질적인 리해를 가지는것이 필수적인 전제로 된다.

INFOSEC 304 UNIX보안

간단한 해설 이 실체험과목에서는 강습생들이 UNIX조작체계에 보안을 실현하는데 필요한 지식과 기술기능을 체득하게 될것이다. 여기서는 내부와 외부의 위험으로부터 체계의 보안, 유닉스파일체계의 보호, 운용관리자접근조종, 취약성을 최소화하고 침입자를 색출하기 위하여 도구프로그람들의 구성문제를 배울수 있다.

강습대상 이 과정안은 유닉스조작체계를 리용하는 망의 설치, 구성, 관리를 책임진 종업원들을 위한 과정안이다. 여기서는 정보관들, 체계관리자들과 체계담당일군들이 학습할수 있다.

강습내용 UNIX보안개론 ; 안전한 구좌설정 ; 구좌정보보관 ; 뿌리접근조종 ; 등록부 및 파일허가 ; 비법프로그람에서 위험요소의 최소화, TCP/IP와 보안에 대한 리해

주의 강습생들은 INFOSEC 203을 완전히 학습하여 IT보안개념들에 대한 본질적인 리해를 가지는것이 필수적인 전제로 된다.

INFOSEC 305 상급ISSO양성

개괄 이 과정안에서는 ISSO의 임무를 명백히 제시한다. 보안계획, 사고방지계획 혹은 재해복구계획과 IT체계인증의 재검토 ; IT체계사고의 처리와 특정IT보안실례연구문제의 검토 및 평가에 초점을 돌리게 된다.

강습대상 이 과정안은 INFOSEC 205를 완전히 학습하고 ISSO로서 적어도 1년간의 경험이 있는 ISSO를 위한 과정안이다.

강습내용 IT체계보안계획과 사고방지계획의 재검토에 대한 감시임무 ; IT체계사고처리 ; 실례연구

INFOSEC 306 사고처리

개괄 이 과정안에서는 IT체계보안사고처리절차를 설명하게 된다. 여기서는 위험성에 대한 사고들을 분류하는 방법을 밝히는것으로부터 시작하여 조사를 시작하고 진행하는 방법, 지원을 받기 위해 누구와 련계를 가져야 하는가 하는 문제들을 취급한다. 사건해결의 열쇠는 조사중에 설비와 정보가 손상되지 않게 하는것이다. 그러므로 강습생들은 자

산과 정보를 안전하게 보관하는 해당 절차를 배우게 된다.

강습대상 이 과정안은 IT보안사건취급을 담당한 종업원들을 위한 과정안이다. 이 종업원들가운데는 정보관, 정보체계보안관, 보안관, 콤퓨터사고에 우려를 표시하는 사람들이 속한다.

강습내용 IT체계보안사고의 리해；련방법률과 민사법적 및 형사법적제재；기관방책 및 형벌；보안조사절차；조사당국의 식별；법집행기관들과의 련계, 보증인면담, 증거보호, IT체계보안사고보고서작성법

주의 강습생들이 INFOSEC 205를 완전히 학습하여 IT보안개념들에 대한 본질적리해를 가지는것이 필수적인 전제로 된다.

INFOSEC 307 위험분석 또는 평가방법

개괄 이 과정안에서는 위험분석 및 평가공정을 취급한다. 여기서는 위험분석의 중요성, 위험분석목적, 위험분석의 가장 적절한 시기, 위험평가(전자도구의 검토)를 위한 각이한 방법들을 개괄하며 많은 실체험기회를 보장하여 본보기위험분석을 완성하게 한다. 위험분석 및 평가의 결정적요소는 목표분석과 목표평가이다. 불법침입자가 정보체계위험분석을 진행하여 공격하기 쉬운 약점들을 알게 될수도 있다.

강습대상 위험분석을 완성할 임무를 맡은 사람들. 정보관, 체계관리자, 프로그람관리자, 정보체계보안관과 보안관이 여기에 속할수 있다.

강습내용 위험분석개관；IT체계들의 취약성；위험 및 민감도와 효과적인 대응책들에 대한 리해；위험분석의 목적；위험분석방법들；위험분석진행에 대한 련방의 지도；위험분석진행공정；전자적인 위험분석도구들；본보기위험분석표(자산가치, 위험 및 취약성의 평가, 위험수준, 대응책)의 완성；목표분석 혹은 평가의 재고찰

주의 이 과정안을 취급하면서 INFOSEC 201과 INFOSEC 206도 배합하여 리용할수 있다.

제２０장. 방책개발

크리스 해어

이 장에서는 기관들에서 왜 보안방책을 세우는가 하는 문제를 취급한다. 방책의 구조, 형식, 절차, 표준 및 지침을 론의하지 않고 방책이 왜 필요한가와 공식적 및 비공식적보안방책, 보안모형 및 보안방책의 형식을 고찰하게 된다.

기관문화의 영향

방책개발문제를 고찰할 때 기관문화가 매우 중요하다. 작업장은 사람들이 일하는 단순한 장소가 아니다. 작업장은 사람들이 맡은 일을 수행할뿐아니라 서로 교제하고 자기들의 직업과 생활에 대하여 자유롭게 의견을 교환하기 위하여 모이는 장소이기도 하다.

방책을 세울 때 이런 문제를 고려하는것이 중요하다. 기관을 더 개방하면 할수록 무거운 제재방책은 종업원들에게 그만큼 더 어렵게 접수될것이다. 문화가 더 제약되면 될수록 즉 종업원들사이에 그들이 관심하는 문제에 대한 의견교환을 그만큼 더 적게 할수록 방책에는 그만큼 더 엄격한 제재조건이 반영될수 있다. 또한 방책의 어조나 초점은 보다 연할수도 있고 보다 강할수도 있다.

종업원들의 호상의견교환수준에는 관계없이 일상조작을 정확히 문서화한 기관은 거의 없다. 이 극단적인 작업환경을 방책에 포함시키기는 어려운것이다. 그러나 이런것은 훌륭한 보안조작에는 더없이 필요한것이다.

보안방책의 력사

보안방책은 보안목적을 달성하기 위하여 기관의 자원을 어떻게 관리, 보호, 할당하는가 하는것을 규제하는 실천조항들로 이루어 진다. 이 보안목적들은 기관의 목표와 환경에 조화되여야 하며 기관이 보안목적을 적용하게 될 방법을 결정해야 한다. 기관의 목표와 보안목적은 서로 결합되여야 사기행위와 사람의 실수와 련관된 위험을 경감시키는 거의 모든 기업실천에 적용된 관리조종을 안받침하게 된다.

보안방책들은 점차로 전개되여 나가며 보안원리들에 기초하고 있다. 이런 방책들은 반드시 기술적인것으로 되는것은 아니지만 그 방책을 지침으로 하면 체계를 실현하는데 사용되는 기술과 밀접히 련관된다.

보안모형들

보안방책은 경영진에 의하여 이루어 지는 결정이다. 어떤 경우에는 보안방책이 보안

모형에 의존한다. 보안모형은 방책과 기술을 실현하는 방법을 규정한다. 이 모형은 전기간 확인된 전형적인 수학적모형이다. 이런 수학적모형으로부터 방책을 개발한다. 모형이 창조되면 그것을 비공식적보안모형이라고 부른다. 모형이 수학적으로 확인되면 공식적인 모형으로 된다. 모형의 확인과 관련된 수학은 이 장의 범위를 벗어 나므로 여기서는 론의하지 않는다. 이런 공식적인 세개의 보안모형으로서는 Bell–Lapadula보안모형 및 Biba보안모형과 Clark–Wilson보안모형들이다.

Bell–Lapadula모형 Bell–Lapadula 즉 BLP모형은 정보보안을 위한 비밀성에 기초한 모형이다. 이 모형은 실현의 기초로 되는 추상적인 모형인바 가장 대표적인것은 국방성(DoD)의 오렌지책(Orange Book)이다. 모형은 한 보안상태로부터 다른 보안상태에로 체계를 옮기는 특정한 변환기능을 가진 안전상태의 개념을 규정한다. 모형은 읽기 및 쓰기와 관련된 기본접근방식과 당사자가 대상에 접근하는 방법을 규정한다.

안전한 상태는 작성된 보안방책에 따라 당사자가 대상에 접근하는것과 같은 오직 승인된 접근방법들만이 리용되는 경우이다. 보안보존에 관한 개념은 이런 상태에서 성립된다. 이것은 체계가 안전한 상태에 있을 때 새로운 규칙을 적용하면 체계를 또 다른 안전한 상태에로 옮기게 될것이라는것을 의미한다. 이것은 체계가 한 안전한 상태로부터 또 다른 안전한 상태에로 넘어 가는 경우에 중요하다.

BLP모형은 당사자와 대상과 련관된 통과허가수준에 기초한 접근을 식별하며 다음에는 읽기전용, 읽고 쓰기 혹은 쓰기전용접근만을 식별한다. 모형은 접근의 두가지 특성을 기초로 한다. 단순한 보안특성 즉 SS특성은 읽기접근특성이다. 이것은 대상이 당사자보다 분류수준이 더 높은 자료를 읽을수 없다는것을 제시한다. 이것을 《no–read–up》(그 이상 읽을수 없음)이라고 한다. 둘째 특성은 별특성 즉 *특성이라고 하는데 읽기접근과 련관된다. 당사자는 분류수준이 같거나 높은 대상에만 정보를 기록할수 있다. 이것을 《no–write–down》(그 이하는 기록할수 없음) 혹은 《제한특성》이라고 한다. 이런식으로 당사자는 한 기밀급에서 다른 낮은 기밀급에로 정보를 복사하지 못하게 할수 있다.

이런것은 좋은것이기는 하나 매우 제한적이다. 대상의 전체와 일부를 식별할수 없다. 모형자체로는 분류를 변화시킬수 없다.

당사자가 임의의 대상에 특정한 접근방법이 어떤것이라는것을 규정하기때문에 BLP 모형은 임의의 보안모형이다.

Biba모형 Biba모형은 무결성모형에 대한 첫 시도였다. 무결성모형이 흔히 비밀성모형과 충돌하게 되는것은 이 두 모형을 균형잡기가 쉽지 않은것과 관련된다. Biba모형은 실세계보안방책과 직접 련관되지 못하기때문에 많이 사용하지 못하였다.

Biba모형은 그 요소들이 한조의 당사자들(능동적인 정보처리를 하는)과 한조의 피동적인 정보보관대상들인 무결성준위와 같은 계층적격자에 기초한다. Biba모형의 목적은 무결성이라는 첫째 목표를 실현하는것이다. 다시 말하여 비법사용자가 정보에 수정을 가하지 못하게 하는것이다.

Biba모형은 BLP와 같은 수학적모형이다. 낮은 준위의 읽기에 의해 정보의 비밀성이 상실될수 있는것과 마찬가지로 무결성모형에서 낮은 준위의 읽기에 의해 높은 준위의 무결성이 떨어 질수 있다.

BLP모형과 류사하게 Biba모형은 ss–특성과 *–특성을 리용하여 제3특성을 보충한다.

ss–특성은 당사자가 무결성이 더 적은 대상을 접근하거나 관찰하거나 읽을수 없다는것을 제시한다. *–특성은 보다 높은 무결성을 가진 대상을 수정 혹은 기록할수 없다는것을 제시한다. 제3특성은 청원특성이다. 이 특성은 당사자가 통보문(즉 봉사에 대한 론리적 요청)을 보다 높은 무결성대상에 보낼수 없다는것을 제시한다.

Clark–Wilson모형 Biba와는 달리 Clark–Wilson모형은 3가지 무결성목표들을 다 다룬다.

- 비법사용자가 수정을 가하지 못하게 하는것
- 내적 및 외적일관성을 유지하는것
- 합법사용자가 부정수정을 하지 못하게 하는것

주의: 내적인 일관성이란 프로그람이 매번 수행될 때마다 예견된대로 정확히 시동한다는것을 의미한다. 외적인 일관성이란 프로그람자료와 실세계자료가 일치한다는것을 의미한다.

Clark–Wilson모형은 잘 이루어 진 거래에 의거한다. 이것은 내적 및 외적일관성요구들을 보존할수 있도록 충분하게 구조화되고 제약된 거래이다. 이것은 또한 셋째 무결성목표와 외부일관성을 실현하기 위한 임무의 분할을 요구한다. 이를 위하여 조작은 소부분들로 나누어 지고 서로 다른 인원 및 공정은 각각 하나의 소부분에 대한 책임을 맡게 된다. 이렇게 하여 주입된 자료가 체계밖에서 리용될수 있는 정보와 일치하게 할수 있는것이다. 이렇게 되면 또한 사람들이 승인없이 변화시키지 못하게 할수 있는것이다. 다른 부분은 보안방책들이다.

표 20－1은 BLP와 Biba모형들의 특성들을 비교한것이다. 이 공식적인 보안모형들은 다 그것들이 매 모형의 목적들을 실현할수 있다는것을 수학적으로 확증하여 보여 주었다. 이 보안모형들은 같은 부분은 일부이고 다른 부분은 보안방책들이다.

표 20－1 BLP와 Biba모형의 특성들

특 성	BLP모형	Biba모형
ss–특성	당사자는 보다 높은 부류의 대상에 대한 읽기 또는 접근을 할수 없다(그이상 읽을수 없음).	당사자는 보다 낮은 무결성수준의 대상을 관찰할수 없다.
*–특성	당사자는 같거나 혹은 보다 높은 부류의 대상만을 보관할수 있다(그 이하로 기록못함).	당사자는 보다 높은 무결성수준의 대상을 수정할수 없다.
청원특성	리용되지 않는다	당사자는 보다 높은 무결성수준의 대상에 론리적봉사요청을 보낼수 없다.

보안방책

1992년에 경제협력개발기구(OECD)는 법률, 방책, 기술적 및 행적적조치와 교육에 대한 일련의 개발지침들을 발표하였다. 이 지침들은 다음과 같은것들이다.

1. **책임.** 정보보안에 인입된 사람들은 자기들의 행동에 대한 특정한 책임을 져야 한다.
2. **의식.** 누구나 다 보안조치, 실행문제와 절차에서 필수적인 지식을 소유할수 있어야 한다.
3. **도덕.** 정보체계와 그와 련관된 보안절차가 리용되는 방법은 사적비밀, 권리 및 다른 사람들의 합법적리익을 존중할수 있어야 한다.
4. **여러 전문분야의 방책.** 방책과 기술의 개발에서 모든 분야의 의견을 고려해야 한다. 여기에는 법률, 기술, 행정, 상업, 교육, 기관 및 운영분야의 의견들이 포함된다.
5. **균형.** 보안조치들은 정보의 가치와 해당 위험수준에 기초해야 한다.
6. **통합.** 보안조치들은 통합하여 함께 작용하도록 해야 하며 보안체계에서 방어심도를 구축해야 한다.
7. **시기성.** 보안위반이 생겼을 경우 모든 사람들은 다 함께 보조를 맞추어 신속하게 행동하여야 한다.
8. **재평가.** 보안절차와 필요성은 주기적으로 재평가되여 기관의 필요성을 실현하여야 한다.
9. **민주주의.** 정보와 그것이 보관되는 체계의 보안은 그 정보의 합법적리용 및 전송과 보조를 맞추어 진행되여야 한다.

OECD보안방책외에 방책을 규정할 때 몇가지 보충방책들을 명심하는것이 중요하다. 이 방책들은 다음과 같다.

10. **개인책임.** 개별적인 사람들은 다 오직 보안체계의 성원으로 간주되며 사용자들은 자기들의 행동에 대하여 책임진다.
11. **인증.** 사용자의 확인 및 인증에 기초하여 특정한 정보 혹은 체계에 접근할 권한을 부여할수 있게 보안조치가 취해 져야 한다.
12. **최소의 특전.** 개별적사람들은 자기의 작업임무를 완성하는데 필요한 정보에만 그리고 그들이 그런 작업을 하는 조건에서만 정보에 접근할수 있어야 한다.
13. **임무의 분담.** 사람들에게 기능을 분담하여 단 한사람도 부정행위를 할수 없도록 해야 한다.
14. **검사.** 수행되는 작업과 그와 련관된 결과들을 감시하여 설정된 절차를 지키고 진행하는 작업을 정확하게 하도록 하여야 한다.
15. **예비조성.** 필요한 경우에 정보들에 접근할수 있도록 해야 한다. 실례로 한 체계가 쓸수 없게 되는 경우에 다른 체계에 정보를 복사하여 계속 접근할수 있게 해야 한다.
16. **위험경감.** 한 사람이 위험을 완전히 제거할수 있다고 말하는것은 비실천적이다. 그러므로 가능한껏 위험을 경감시키는것을 목적으로 한다.

실세계보안방책에는 방책을 작성하고 실현할 때 고려해야 할 중요한 일련의 역할들이 있다. 이 역할들은 방책의 각이한 요소들을 실현하는데서 나서는 요구들사이의 차이

점들을 밝혀 주므로 중요한것이다. 이런 역할들은 다음과 같다.

1. **발기자** 정보를 만드는 사람
2. **위임자** 정보접근을 관리하는 사람
3. **소유자** 우의 두 역할을 겸비하였거나 겸비하지 못한 사람
4. **보호자** 정보접근을 관리하며 정보접근과 관련한 위임자의 의도를 수행하는 사람
5. **사용자** 작업임무를 완성하기 위하여 정보접근을 최종적으로 원하는 사람

중요보안목표들(비밀성, 무결성 및 리용성)을 보면 보안방책들은 흔히 처음 두 목표 즉 비밀성과 무결성을 위주로 작성된다. 비밀성은 정보의 비밀 및 접근에 관한것이다. 비밀성에서는 또한 보호된 정보에 대한 비법접근, 수정 및 파괴에 관한 문제를 취급한다. 무결성은 정보수정을 방지하며 수신인이 정보를 요구할 때 정확하게 정보를 받을수 있게 하는 문제에 관한것이다.

흔히 이 두 목표는 서로 다른 목적으로 하여 충돌하게 된다. 앞에서 언급한바와 같이 Bell–Lapadula모형은 비밀성을 다루는데 이것은 우연히도 국방성이 개발한 신뢰성콤퓨터사용표준평가기준의 목적이기도 하다.

리용성은 필요한 경우에 정보를 항상 리용할수 있게 하는데 기본을 두고 있으므로 다른 문제에 속한다. 보안이 이 목표에 영향을 주지만 정보의 리용성에 긍정적 및 부정적영향을 줄수 있는 다른 여러가지 요인들도 있다.

《만리장성》(Chinese Wall)방책은 그것으로서는 공식적인 보안모형으로는 되지 못하지만 알아둘 가치는 있다. 이 방책에서는 리해의 충돌중심으로 정보를 그 급에 따라 분류한다. 사람들은 자기들의 작업기능을 수행하기 위하여 의뢰기내부운영과 관련된 정보에 자주 접근할 필요가 있다. 그렇게 하여 같은 기업의 다른 의뢰기들에 의견을 주게 되면 그것들은 리해의 충돌에 직면하게 된다. 정보를 그 급에 따라 분류하면 공급자는 의뢰기와 관련된 다른 정보를 알수 없다. 《만리장성》(Chinese Wall)방책은 법률분야와 회계분야에서 종종 쓰인다.

그러나 보안방책의 범위는 매우 넓다. 성과를 거두자면 보안방책이 가동하는 기술적인 실천에 신뢰성 있게 정확하게 구현되여야 한다. 보안방책은 모호하지 않게 구체적으로 문서화되여야 한다. 그렇게 되지 않아 그것을 사람이 일일이 따라가며 해석해 주게 되면 그 해석이 입력된 자동화된 체계는 정확히 동작하지 않을수도 있다. 이로부터 방책규정을 가능한껏 구체화하는것이 절대적으로 필요한것이다. 오직 이렇게 할 때 보안방책의 자동적인 실현이 성과적으로 된다.

또한 콤퓨터사용정황과 관련하여 몇가지 방책선택을 해야 한다. 이 방책선택에는 콤퓨터관련장치의 보안과 사용자들이 어떻게 자기들을 식별하는가 하는 문제들이 포함된다. 비밀성과 무결성을 성과적인 보안방책에서 결합하는것이 어렵다는것을 기억할 필요가 있다. 따라서 성문화된 방책을 자동적인 체계에로 전환할 때 실현단계에서 문제성이 생길수 있다. 기관의 실세계보안계획은 기관의 목표들을 반영하여야 한다.

방책자체가 실천적이여야 하며 리용할수 있어야 한다. 방책은 비용의 효과성이 높아야 한다. 다시 말하여 방책실현비가 보호되는 재부의 가치보다 높지 말아야 한다. 방책

에는 보안실현의 구체적인 표준이 반영되여야 하며 오용에 대한 대응이 밝혀 져야 한다. 방책은 사용자들이 리해할수 있도록 명백하게 서술되여야 하며 은어가 없어야 한다. 무엇보다도 높은 급의 경영진에 대한 지원을 해야 한다. 이런것이 없으면 심지어 제일 훌륭한 보안방책도 실패하게 될것이다. 방책에 보안과 사용상의 편의를 반영하는것이 또한 대단히 중요하다. 사용법이 너무 힘들어서 사용자들이 자기 일을 수행할수 없게 한다면 기업에 부정적인 영향을 주어 사용자들로 하여금 보안실현을 하지 않고 에돌아 가게 한다. 다른 한편 사용상의 편의에 너무 치중하면 기관의 보안자세에 영향을 주어 가능한 보안의 수준을 떨구게 될수 있다.

방책은 왜 필요한가

사람들은 장기적보안이 필요하다는것을 리해하였다. 한 사람이 다른 사람에게 필요한 가치 있는것을 가지고 있은 때로부터 사람들은 보안을 그 재부보호의 필요성과 련결시켰다. 대부분의 사람들은 은행에서 금고실과 안전금고를 리용하여 돈과 중요한 문서를 관리하는 방법에 익숙해 졌다. 은행이 해당 보호절차들을 실행하는 방법을 제시한 방책을 가지고 있지 못한다면 대중은 은행에 대하여 신뢰할수 없게 될것이다.

보안자체는 오랜 력사를 가지고 있다. 콤퓨터는 최근에야 그런 보안의 력사에 들어서게 되였다. 사람들은 문에 쇠를 설치하여 도적이 쉽게 들어 오지 못하게 하였다. 사람들은 은행과 다른 기술을 리용하여 가치 있는것, 집과 가정들을 보호한다. 군대에서는 적들로부터 자기 정보를 보호할 필요성을 이미 오래전부터 느꼈다. 이로부터 통보문을 암호화하는 암호학을 개발하여 적들이 암호문을 읽지 못하게 하였다.

많은 보안기술과 방책은 개별적인 한 사람이 부정행위를 혼자서 하지 못하도록 하는데 목적이 있다. 또한 보안기술과 방책은 적절한 정황에서 감시통제를 보장하는데도 쓰인다.

통제의 필요성

방책은 기관의 사람들이 무엇을 할것인가 하는것을 알게 하는데도 필요한것이다. 이에 대한 일련의 각이한 리유들 즉 법적순응, 주권소유자의 신뢰유지, 기관에서 목적들을 세우고 유지할수 있다는것을 종업원들에게 보여 주는 문제 등이 있다.

방책과 절차의 수립을 필요로 하는 많은 법적요구들이 있다. 이 요구들에는 성실성과 조심성도 포함된다. 성실성은 일정한 법적개념들에서 즉 공정성, 리해의 충돌, 기업기회와 비밀성 등에서 명백히 나타난다. 리해충돌의 정황을 피하기 위하여 개별적사람들은 기업소의 리익에 간섭할수 있는 그 어떤 외부적관계도 밝혀야 한다. 공정성에서는 리해관계의 충돌이 있게 될 때 개별적사람은 모든 당사자들의 리익에 완전히 부합되게 행동할 의무를 지닌다.

병합, 획득 및 특허품 등에 대한 사전통고와 같은 물질적인 내부정보가 제시될 때

개별적사람은 그것들을 개인적인 벌이에 리용하지 말아야 한다. 이렇게 하지 않는 경우에는 회사의 좋은 기회를 망쳐 버리는 결과를 가져 온다.

운영상문제가 제기되는 사고가 있을 경우에 이런 요소들은 영향을 미치게 된다. 효과적인 준수과정을 제대로 갖추어 회사가 방책, 절차와 표준을 제대로 리용하게 하는것은 회사에 대한 형사조사를 진행하는 경우에 긍정적인 효과를 낼수 있다. 실례로 준수과정에 고유한 대부분의 기초기능들은 다음과 같다.

- 방책, 절차 및 표준을 세워 로동력을 지도하는것,
- 높은 급의 관리자를 임명하여 방책, 절차 및 표준의 준수를 감시하는것,
- 종업원들에게 임의의 권한을 줄 때 응당한 주의를 돌리는것,
- 모든 종업원들에게 표준과 절차를 알려 주는것,
- 알맞는 징벌조치들을 통하여 방책, 표준 및 절차들을 일관하게 실시하는것,
- 준수사항들을 위반한 경우에 정정 및 수정절차들을 집행하는것.

법적견지에서 본 세번째 요소는 1996년 경제정탐행위관계법(EEA)이다. EEA는 처음으로 무역비밀정보를 훔치는것을 련방범죄로 규정하였으며 범죄들에 벌금, 감금 및 몰수와 같은 형벌을 적용하였다. 그러나 EEA는 또한 정보를 가지고 있는 기관들에서 리성적인 노력을 기울여 정보를 보호하리라고 기대하고 있다.

법률적요구사항뿐만아니라 방책과 절차들을 세워야 한다는 훌륭한 기업적리유도 있다. 재정적재부를 보호하는것이 중요한것처럼 기관에 그렇게 중요한 정보를 보호하는것이 중요하다는것은 잘 알려 진 사실이다. 이것은 종업원들, 판매자들, 고객들 및 다른 합법적망사용자들에 대한 통제가 필요하다는것을 의미한다. 지구상의 임의의 지역에서부터 정보에 접근하려는 요구가 늘어 나므로 정보보안방책, 절차 및 표준을 기관적인 규모에서 잘 세우는것이 중요하다.

호스트형체계로부터 의뢰기/봉사기형체계까지의 콤퓨터리용환경에서 많은 변화가 일어나면서 그러한 환경보호의 복잡성은 급속히 늘어 났다. 결론적으로 말하여 통제를 잘하면 기업의식이 좋아 진다. 방책과 절차들을 잘 실행하지 못하면 사고가 생겨 사회적으로 알려 지는 경우에는 회사에 대한 주주들과 시장의 신뢰가 떨어 지는 결과를 가져 오게 된다.

방책과 절차를 성문화할 때 회사의 임무, 가치, 기업운영에 대한 확고한 인식을 가지는것이 필요하다. 기관을 보호하는데 필요한 통제항목을 규정하고 설정하기 위하여 방책과 절차가 필요하다는것과 보안을 위한 보안은 회사와 그 종업원 또는 그 주주들에게 의의가 없다는것을 잊지 말아야 한다.

가장 훌륭한 관례의 모색

변화가 생기고 기업이 발전함에 따라 방책을 재고찰하고 그에 기초하여 기업의 필요성을 계속 실현시키는것이 필요한것이다. 그러나 기관들이 다른 기관들과 련계를 가지고 가장 훌륭한 관례와 관련된 정보를 교환하는것이 또한 좋을것이다. 모든 기관들에서는 부단한 갱신을 중요한 목표로 하여야 한다. 가장 훌륭한 산업관례에 대한 재검토는 기관

들의 성능비교검사이기때문에 그 산업개선의 중요한 부분으로 된다.

어떤 기관에서는 특별한 방책을 자기식으로 실현하려고 하지만 다른 기관에서는 완전히 다른 식으로 할수도 있다. 보안기관들은 정보를 공유함으로써 자기들이 개발한 방법들을 개선하고 업계에서 정보전달을 유지할수 있다.

한 회사가 다른 회사로부터 어떤 문제가 합당하며 어떻게 하는것이 좋겠다는 의견을 말할수 있는 회합들은 많다. 어떤 문제를 택하며 어떻게 하는것이 좋겠다는 의견을 회사들이 서로 나눌수 있는 여기에는 토론연단들이 많다. 콤퓨터보안연구공동작업연단과 국제정보무결성강습회(I–4)도 여기에 속한다. 콤퓨터관련설비협회(ACM)와 같은 공학기관들이 주최하는 기타 특수한 리익단체들도 있다.

그 어느 경우에나 가장 훌륭한 관례를 마련하자면 구성요소의 제작이건 보안방책의 실현이건 시간이 많이 걸린다.

관 리 임 무

방책의 작성과 집행에서 경영진은 특별한 책임을 지닌다. 여기에는 방책명시, 방책실천능력소유, 방책통보 그리고 방책의 작성 및 집행에 필요한 자원을 보장하는것이 속한다. 그러나 경영진은 기관의 물리적 및 정보재부의 보호에 대하여 립법부, 종업원, 주주들앞에 최종적으로 책임진다. 이런 책임을 다하기 위하여 경영진은 기관의 운영과 기관의 사업방법을 제시하게 되는 방책작성에서 견지해야 할 일정한 법적원칙들을 가진다.

성실성의 의무

매 사원은 사업에서 솔직, 성실, 절대적신뢰라는 법적인 의무를 지니고 있는데 여기에는 리해관계의 충돌과 사리를 추구하지 않는것도 포함된다. 매일 자기 사업을 책임적으로 수행하는데서 사원들은 비법적이 아닌 이상 언제나 회사의 리익에 가장 잘 부합되게 행동하여야 한다. 사원의 리익을 회사의 리익우에 올려 놓는것과 같은 탈선행위는 그 어떤 형태이든지 성실, 조심, 절대신뢰라는 사원의 의무에 대한 위반행위로 간주될수 있다. 신용 있는 사원들은 보통의 사원들보다 더 높은 수준의 조심성을 발휘하게 된다.

어떤 부서책임자가 자기 부서 사원이 자기 리익을 회사의 리익보다 우선시하는것을 알고 있는 경우 그 부서책임자는 좋기는 서면으로 그 사원에게 회사앞에 지닌 도리를 충고식으로 알려 주어야 한다.

리해관계의 충돌

리해관계의 충돌이라고 하면 일부 사람들에게는 리익을 주지만 다른 사람에게는 해를 준다는것을 충분히 알면서도 어떤 결정을 내리는 경우라고 할수 있다. 실례로 두 대방이 서로 리해관계상 충돌이 있는데 그것을 알면서도 두 대방을 같이 말아 보는 변호사

가 있다고 하면 그 변호사는 리해관계의 충돌에 빠져 있는것이다.

조심성의 의무

조심성의 의무는 지휘성원들이 자기들에게 맡겨 진 중요한 과업을 수행할 때 조심스럽게 행동해야 할 의무이다. 실례로 리사는 조심스럽고 신중하게 회사의 리익에 가장 잘 부합되게 자기 임무를 수행하여야 한다.

더우기 경영자들과 그 아래사람들은 자기들의 임무를 모른다 하더라도 체계를 보안하며 기억된 전자정보를 보호해야 할 책임을 지니고 있다. 자기 책임을 모르는 이런 문제는 다른 나라들의 일반법에 서술된 바와 같이 파실문제로 된다.

기관에서 문제가 생긴다 해도 기관이 책임을 다는 지지 않을수도 있다.

기관에서 다음과 같은것 즉

- 적절한 사전대책을 취하였다,
- 흔히 쓰이는 통제수단 및 관례를 적용하였다,
- 보통 요구되는 보안통제목적에 맞게 한다,
- 잘 가동하는 콤퓨터설비에 리용될수 있는 방법들을 적용한다,
- 상식과 신중한 경영상 관례를 적용하였다

는것을 보여 줄수 있다면 기관에서도 응당한 조심성을 가지고 운영하였다고 말할수 있을것이다.

최소의 특권

최소특권의 개념은 그 기능을 수행하는데 실제로 필요되는것보다 더 많은 특권을 매 공정이 가지지 않는다는것을 의미한다. 《감독》접근 혹은 《뿌리》접근(즉 완전한 체계특권)을 요구하는 모듈들은 핵심부에 끼워 진다. 핵심부는 체계자원에 대한 모든 요구들을 다루며 필요한 경우에 외부적인 모듈들이 특권모듈들을 부르도록 허락한다.

임무/특권의 분할

임무의 분할은 사람에게 적용된 술어이지만 특권의 분할은 체계에 적용되는 술어이다. 특권분할은 둘 또는 그이상의 장치들이 일치해야 공정이나 자료 혹은 체계요소들의 잠금상태가 해제된다는것을 보여 주기 위하여 쓰인 술어이다. 이런식으로 접근을 얻기 위해서는 두 체계공정사이의 일치가 있어야 한다.

책임관계

책임관계는 특정한 개인이 자기 행동에 대하여 책임 지는 능력이다. 개인에게 책임

을 지우기 위하여서는 그 사람을 유일하게, 효과적으로 식별인증할수 있어야 한다. 이것은 기관에서 매 개인을 유일하게 식별하는 방법을 실현하지 못한다면 매 개인에게 자기행동에 대하여 책임지울수 없다는것을 의미한다. 두가지 큰 주제 즉 (1)사용자가 체계에 접근할 때 그 개인에 대한 식별 및 인증 ; (2)개인이 특정한 거래를 발기하였거나 요구하였다는 확인이 있다.

방책에 대한 경영측의 지원

새로운 제품 또는 봉사의 개발이건 방책의 작성이건 그 어떤 발기에서도 성과의 결정적요인은 경영측의 지원이다. 상급경영측이 행동의 의도를 승인하지 않으면 그 행동은 성공할수 없을것이다. 이것은 기관의 보안방책작성에 한한 문제가 아니며 어떤 행동에도 다 해당되는 문제이다. 그러나 보안방책은 모든 기관에서 중요한 문제점들을 제기할수도 있으며 처리할수도 있다. 경영자의 지원을 받는것은 종종 계획화공정의 가장 어려운 부분이다.

방책계획화

계획화와 준비는 방책, 표준 및 절차작성의 전일적인 부분들이지만 종종 무시 당한다. 준비공정에는 수행하여야 할 모든 사업이 포함된다. 방책은 취해야 할 일반적인 요구들을 제시한다. 표준들은 사용될 도구들을 규정한다. 절차들은 방책을 수행하기 위한 구체적인 지령들을 종업원들에게 보장한다.

성문화가 잘된 절차들이라해도 감독을 대신하지 못하지만 그것들은 보다 현실적인 과업을 제기하여 종업원들이 수행하도록 한다. 종업원들은 경영자들과 토론할수 없는 경우에 결심을 채택할 때 방책을 리용하여 정보와 지침을 보장한다. 방책에는 누가 어떤 행동에 대하여 책임진다는것을 식별해 놓아야 한다.

효과적인 방책조항들은 기관에서 두가지 중요한 요구 즉 임무의 분담과 과제의 순환식제시를 수행할수 있도록 실제로 도와 줄수 있다. 개별적인 한 사람이 시작으로부터 완성에 이르기까지의 완전한 공정에 대한 완전한 통제를 할수는 없다. 통제는 협잡행위로부터 기관을 보호하는 하나의 요소이다.

방책작성기간의 계획화에는 보안원칙에 대한 주의를 돌리는 문제가 포함되여야 한다. 실례로 세심한 주의를 요하는 업무를 맡은 사람들은 주기적으로 순환하면서 다른 임무를 맡아야 한다. 이렇게 하면 사람들은 긴장한 조작에서 벗어 나게 되고 작업의 긴장도는 줄어 들게 된다. 순환식임무수행은 일의 효과성과 개선을 비롯한 일련의 효과를 달성하게 한다. 개선의 측면은 사람들이 일을 번갈아 할수 있게 하며 시야를 넓혀 주고 작업에서 실수를 방지하여 작업결과의 질을 높이게 하는것이다.

방책이 작성되면 그 방책을 지원하는데 쓰일 표준을 규정하는것이 필요하다. 이 표준들에는 하드웨어, 쏘프트웨어 및 통신규약이 포함되여 있다. 종업원들과 다른 사람들

에게 정보를 보내주기 위하여 작성된 통보계획이 없이는 이런 단계들을 거쳐 준비하여도 아무 소용도 없게 된다.

경영자들이 모든 종업원들을 일일이 만나 그들의 임무를 알려 줄 시간적여유가 없기 때문에 통보계획이 특별히 중요할것이다. 그러나 경영자들은 모든 사용자들에게 방책의 내용을 끊임없이 알려 주며 종업원들에게 방책수행에서 많은 임무를 인식시킬 책임을 지니고 있다.

종업원들에게 정보를 제공하는 능력은 방책, 표준 그리고 절차의 작성에서 본질적내용의 하나이다. 이런 수단들을 리용하여 종업원들은 방책에 따라 자기 과업들을 어떻게 수행하여야 하는가를 알게 될것이다. 방책과 련관된 문서들을 누가 작성하는가, 그것들을 누가 검토하는가 그리고 포함된 정보에 대한 합의는 어떻게 이루어 지는가 하는 문제들을 설정하는것은 계획화공정의 한 부분으로 된다. 실례로 경영진의 결정을 그 집행도 고려하면서 어떻게 작성할것인가 하는 문제를 론의할 때에는 많은 전문가들이 참가하게 된다. 바로 이 전문가들은 계획작성자들, 경영진 그리고 공동리해관계를 가진 사람들과 협력하여 방책이 현실성 있고 수행할수 있는것으로 되게 한다. 방책을 효과적으로 작성하는 사람들외에 방책이 타당성을 가지도록 하기 위한 보충적인 인원들이 요구된다. 실례로 방책을 재검토하는 전문가들가운데는 인적 및 법적문제들을 담당한 사람들도 있게 된다.

방책관리계층

방책관리계층에는 5개의 단계가 있다. 이 단계들은 그림 20−1에서 설명된다.

제1단계인 법률단계에서는 기관의 규모에 관계없이 기관에 대한 영향력을 행사한다.

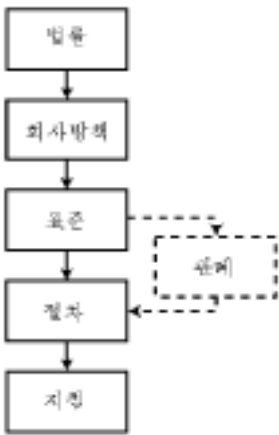



그림 20−1. 방책관리계층

그 영향은 리익금과 세금으로부터 시작하여 수출통제자료에 이르기까지 다 포괄한다. 법률은 정부에서 제공하며 법률에 따라 취해 진 방책은 법률에 의하여 실시되거나 실시되지 않을수도 있다.

제2단계에서는 기관에서 작성하고 고위경영측이 승인하는 방책을 취급한다. 방책에는 기관에 대한 그 중요성이 밝혀 져 있다.

제3단계에서는 방책에 따라 설정되는 표준을 취급한다. 표준에는 그 준수정형을 립증하는데 사용할수 있는 특정한 측정값들이 제시되여 있다.

제4단계(절차)에서는 방책과 표준을 실현하기 위하여 어떻게 해야 한다는 지령들을 차례로 제시한다.

제5단계(지침)에서는 기관성원들이 수행해야 할 작업정형을 립증하게 된다. 우의 단계들에서는 흔히 권고의 형식을 취하며 표준단계에서는 지시의 형식을 따르지만 지침단계에서는 선택방법으로 한다.

표준과 절차사이에 삽입되는 하나의 보충단계가 있을수 있다. 이 단계에서는 하나의 흐름과정에 비길수 있는 관례를 취급한다. 표준단계에서는 수행되여야 할것을 제시하고 관례단계에서는 리유와 방법을 규정한다. 그러나 절차단계에서는 실현에 대한 특정한 하나하나의 지령들을 제공한다. 작성형식과 방법을 비롯하여 우의 문서들에 대해서는 이 장의 뒤부분에서 언급한다.

방책의 류형

방책의 류형에는 3가지 즉 규제, 권고 및 통보가 있다. 기관에서는 기관전체에 적용할수 있는 해당 방책을 작성할수 있지만 산하부서들에서는 부서내방책을 자체로 작성보급할수 있다는것을 알아 두는것이 또한 중요하다.

규제방책

규제방책은 기관에서 허술하게 대하여도 되는것이 아니라 반드시 의거해야 하는 방책이다. 의학과 법률과 같은 일부 전문분야들을 규제하는 정부와 규제 및 통제기관들은 전형적으로 이런 형식의 방책을 세운다. 일반적으로 공동재부의 안전이나 관리와 같은 공동의 리익을 위하여 운영되거나 자기들의 행동에 대하여 집단앞에 책임질수 있는 기관들은 규제방책의 사용자들이다.

이런 류형의 방책은 무엇을 수행하여야 하는가, 언제 수행하여야 하는가, 누가 수행하는가를 구체적으로 밝히며 그것을 수행하는것이 왜 중요한가에 대한 명확한 분석을 줄수 있는 일련의 법적조항들로 이루어 진다. 많은 그룹들이 이런 방책들을 리용하기때문에 그들은 자기 기관을 위하여 이런 방책들을 함께 리용하며 해석한다. 비밀성, 무결성 및 리용성(CIA)외에 규제방책을 세우는데는 2가지 전제조건이 있다.

첫째 전제조건은 명백하게 일관한 공정을 세우는것이다. 이것은 일반대중이 일하는

기관들에서 특히 절실한것이다. 그러므로 이런 기관들에서는 편견 없이 규정을 적용하는 일관성을 세워야 한다. 둘째 전제조건은 해당 부문을 책임진 기술지식이 없는 사람들이 그 부문의 과업을 수행할수 있는 기술적능력이 있어야 한다는것을 절감하게 하는 계기를 방책에 반영하는것이다.

규제방책은 흔히 그 적용에서 례외조건들 혹은 제한조건들을 가진다. 규제방책은 사람들이 직면한 사실에 기초하여 결정들을 즉시 만들어야 하는 경우에는 실효성이 없는것이다. 이것은 많은 정황들이 많은 각이한 결과들을 가져 오는 사정과 관련된다. 모든 가능한 결과들을 처리할수 있는 방책의 수립은 결국 매우 복잡하며 적용하기 힘들고 또한 실시하기 매우 어려운 방책을 제기하는것으로 된다.

권고방책

권고방책에는 일정한 정황에서 취해 질 행동에 대하여 매우 강한 표현으로 작성한 건의안들 혹은 사용방법이 반영된다. 이것은 방책의 정의에 모순되는것 같지만 현실적으로 권고형식의 방책은 이런 건의안들을 제기한다. 권고방책은 지식 있는 사람들에게 정보를 제공하여 정황 및 행동방식과 관련한 결심을 채택하게 한다.

이 방책은 권고방책이기때문에 그 실행이 어렵지 않다. 그러나 방책의 한계안에서 제공되는 조언을 따르지 않는데서 생기는 후과도 방책에 반영된다. 방책은 해당 후과들을 밝히며 또한 행동방향을 바꾼다면 후과가 어떻게 된다는것을 밝힐 능력을 정보를 접수한 사람들에게 제공하여 준다.

방책을 따르지 않는데서 오는 후과들에는 다음과 같은것들이 있을수 있다.

- 충분한 결심채택에 필요한 정보를 놓치는것,
- 결정채택과 공정완성의 적임자들에게 통지를 하지 못하는것,
- 중요한 최종한계시간을 놓치는것,
- 검열자들 및 경영진과 함께 대안들을 검토평가하는데 시간을 랑비하는것.

권고방책을 따르지 않는데서 오는 위험이 기관들에 큰 문제로 될수 있다고 보는것이 중요하다. 대안의 평가와 토론으로 하여 잃어 버린 생산시간의 비용만이 기관에 그리고 과정의 타당성과 정확성을 평가하는데 큰 타격을 줄수 있다.

권고방책들에는 흔히 일정한 제한조건과 례외조건들이 있다. 실례로 권고방책에는 행동방향결정에 오직 경험 있는 사람들만이 참가할수 있으며 경험이 적은 사람들은 개인적인 결심채택을 허용받지 못하고 규정된 방책을 따라야 한다는것이 제시될수 있다. 방책의 례외조건들과 그런 정황에서 수행되여야 할것을 문서화하는것이 또한 중요하다.

통보방책

제3형태의 방책은 본질상 통보성을 띠는 방책이며 그 목적은 해당 대상들에게 정보를 보내는것이다. 통보대상은 일반적으로 그 방책을 읽을 기회 또는 리유를 가지는 임의

의 개별적인 사람이다. 이 방책에는 독자의 행동이나 책임사항이 제시되여 있지 않으며 또 이 방책을 따르지 않아도 법적제재는 받지 않는다.

통보방책이 규제방책이나 권고방책들보다 덜 중요한 정보를 제공할수 있지만 특정한 정황들에서는 강한 사상을 통보대상들에게 줄수 있다. 통보방책의 대상들이 많은것으로 하여 더 구체적인 다른 방책들을 참고로 하여 더 구체적인 정보를 볼것을 권고할수 있다. 이렇게 되면 보다 기밀적인 내용을 담은 방책들은 그 배포를 제한하고 통보방책들을 배포함으로써 위험성을 줄이게 된다.

회사방책과 부서방책

회사방책과 부서방책의 유일한 차이는 그 범위에 있다. 실례로 기관들에서는 고객들호상간의 관계를 취급하는 방책을 규정할수 있다. 특정한 기관들에서는 일정한 부서에만 있는 고객들호상간의 관계를 취급하는 방책을 밝힐수 있다. 온 기관에 적용되는 방책으로서는 회사 혹은 기관 방책외에 또 다른 방책이 없으며 부서방책은 그 부서에만 한한 방책이다. 범위가 좁기때문에 방책을 재검토하고 그에 대한 의견을 발표해야 할 사람이 줄어 드는 관계로 방책을 재고찰하고 승인하는 과정은 그만큼 짧아 질수 있다.

일정방책과 주제방책

이 중요한 방책형태들은 별개의 문제로 하고 일정방책과 주제방책사이의 차이를 밝혀 주는것이 중요하다. 일정방책은 기관의 전반적보안에 대한 관점을 세우는데 쓰이지만 주제별방책들은 관심사로 되는 특정한 주제들을 제시하는데 쓰인다. 또한 주제방책은 특정한 응용 혹은 체계를 보호하는데 쓰이는 응용별 방책이다.

방 책 작 성

방책의 각이한 형태들, 경영진의 지원과 새방책보급의 중요성 그리고 기관에서 방책의 필요성을 고찰한 후에는 기관을 위한 방책작성과정에로 넘어 가게 된다.

방책의 주제

모든 기관에서는 기본적인 방책들을 다 세워야 한다. 이 방책들은 흔히 기관들에서 문서로 준비할수 있으며 정보보안전문가들은 여기에 필요한 내용들을 보충할수 있다.

어느 한 문제에 대한 상급경영진의 결심에 의하여 방책의 매 조항이 작성된다. 그러므로 방책에 리용될수 있는 주제들의 범위는 넓은것이다.

이 방책에 반영할 주제들은 다음과 같다.

1. 일치한 사상
2. 행동규범
3. 리해의 충돌
4. 통보
5. 전자통신체계
6. 인터네트보안
7. 전자통신방책
8. 일반보안방책
9. 정보보호방책
10. 정보분류

이것은 모든 항목들을 다 포괄하는 목록이 아니지만 문제로 설정되는 분야들을 식별하는데 목적이 있다. 방책의 개발에 착수하기전에 모든 방책주제분야들을 다 식별할 필요는 없다. 하나의 방책을 작성하면서 다른 기관의 방책 혹은 다른 련관된 문서를 참고할수도 있는것이다.

어느 방책에서나 리용해야 할 일정한 형식이 있다. 그러나 기관에서 이미 작성한 방책이 있다면 새로 작성하는 방책을 이미 작성한 방책의 형식에 맞추어 세워야 한다. 이렇게 하는것은 방책을 읽을 때 그것을 방책으로 리해하도록 하기 위하여 중요한것이다. 방책을 작성하면서 종래의것과 다른 형식을 취하면 그것이 방책임에도 불구하고 독자는 그것을 방책이라고 생각하지 못할수도 있다.

보안원칙들이 방책개발에 주는 영향. 기관에서는 방책개발에 의의가 있는 일정한 정도의 보안원칙들을 선택해야 한다. 방책과 련관문서들을 개발할 때 선택한 원칙들을 고려해야 하며 선택한 원칙들에 대한 방책(즉 표준, 절차 및 지침)의 호상관계를 재검토해야 한다. 이것은 표 20－2에서 보여 주는 모형을 실행하는 과정을 통하여 쉽게 수행할수 있다.

표 20－2 원칙의 재검토와 방책의 전개

방책내용	원칙 1	원칙 2
전체 방책내용	이 원칙이 적용되면 이 란에 ○를 넣으라.	이 원칙이 적용되면 이 란에 ○를 넣으라.

이 모형에서 요구되는 원칙들은 모형의 웃부분에 가로 기록하며 방책내용들을 왼쪽란에 내리 기록한다. 《○》는 해당한 란들에 표시하여 원칙과 방책내용사이의 관계를 설명한다. 방책(혹은 방책구성요소)에 원칙들을 련관시킴으로써 방책작성자는 그 성과를 평가할수 있다. 이렇게 되는것은 원칙들이 기관의 목적 즉 업무의 부분으로 되여야 하기때문이다.

어떤 원칙도 반영하지 않는 방책이나 구성요소가 있다면 그 방책 또는 구성요소를

재검토하여 그것이 실제로 필요한가 혹은 요구되지 않는 원칙이 있는가 하는것을 밝혀야 한다. 이런 비교를 진행하여 방책작성자는 방책을 전개하는 도중에 수정을 가하거나 혹은 주요원칙들과 관련하여 상급경영진에 건의할수 있다.

방책작성기법

방책을 작성할 때 작성자가 방책전달대상을 고려하는것은 필수적이다. 이렇게 하는것이 중요한것은 방책전달대상이 리해하지 못하게 작성한 방책은 청중에게 혼란과 오해를 일으킨다는 사정과 관련된다.

언어. 방책전달대상에게 알맞는 언어를 사용하는것은 중요한 문제이다. 은어를 쓰지 말아야 하며 될수록 리해하기 쉬운 말을 해야 한다. 방책을 리해할수 있어야 사용자들은 자기들의 임무와 방책을 실현하기 위하여 해야 할것을 정하게 된다. 흔히 쓰지 않는 언어로 방책을 작성하면 방책이 잘못 해석될수 있다.

초점. 방책에서 취급되고 있는 화제에서 벗어 나면 안된다. 보충적인 화제와 문제들을 방책에 끌어 들이면 방책을 리해하기 어렵게 되고 혼란을 주게 될것이다. 쉬운 어림짐작방법에 의하면 매개 중요한 화제마다에 하나의 방책이 담겨 져야 한다는것이다. 하나의 방책이 너무 크면(즉 4페지 이상이면) 화제내용은 부분화제들로 갈라 지므로 방책의 초점을 놓치지 않으면서 경영진이 의도하는 내용들을 취급해야 한다.

형식

방책은 효과적인 정보보안구조를 구축하기 위한 초석으로 된다. 방책문은 방책이 무엇인가를 규정하며 방책의 가장 효과적인 부분으로 간주된다. 정보보안방책의 목표는 정보자원의 무결성, 비밀성 및 리용성을 유지하는것이다. 기관들이 이 목표를 달성하지 못하게 하는 기본위험들에는 고의적이건 우연적이건 도난, 수정, 파괴 혹은 루설이 속한다.

용어《방책》은 사람마다 각이하게 해석한다. 방책은 어떤 문제에 대한 경영진의 결심이다. 방책은 흔히 기업소의 확신, 목표와 목적 그리고 특정한 문제의 분야에서 그것을 달성하기 위한 일반적수단을 기술한 사항들을 포함한다.

방책문자체는 높은 준위에서 간명하게 규정된다. 방책이 높은 준위에서 작성되기때문에 그 방책을 수행하는 방법을 기록하여야 한다. 방책의 효과성보장에 의무적인 행동, 규칙, 준칙 혹은 규정은 표준대로 되여야 한다.

방책에 포함되지 않은 별지문서인 지침들은 절차작성의 기초틀거리를 제공하는 보다 일반적인 사항들이다. 표준들은 의무사항이지만 지침들은 권고안으로 된다. 실례로 다중인증을 어떤 정황에서 해야 하는가를 밝히는 방책은 기관에서 작성할수 있다. 표준에 의하면 접수될수 있는 다중인증도구에는 접수되고 승인된 방법들에 대하여 특정한 사항들이 명문화되여 있어야 한다.

방책들이 다음과 같이 되여야 한다는것을 기억하라.

1. 리해하기 쉬워야 한다.
2. 적용할수 있어야 한다.
3. 수행할수 있어야 한다.
4. 강제력이 있어야 한다.
5. 단계적으로 수행할수 있어야 한다.
6. 예방적인것으로 되여야 한다.
7. 절대적인것으로 되지 말아야 한다.
8. 기업목적을 실현하여야 한다.

방책을 작성하는것은 쉬울수도 있고 어려울수도 있다. 그러나 방책작성자는 일반적인 방책형식에 구애되지 말고 많은 기자들과 작가들이 의거하는 특성들을 기억해야 한다.

- **무엇**. 방책의 취지는 무엇인가.
- **누구**. 누가 영향을 받는가, 종업원과 경영진의 책임과 의무는 무엇인가.
- **어디에**. 어디에 방책이 적용되는가, 방책의 규모는 얼마나 되는가.
- **어떻게**. 준수요인은 무엇인가 그리고 준수정도는 어떻게 측정하는가.
- **언제**. 방책은 언제 효력을 발생하는가.
- **왜**. 이 방책을 실현하는것이 왜 필요한가.

방책의 특성들을 고찰하는데서 남의 평가를 찾아 보기전에 방책작성자가 방책에 대한 자체평가를 하는것이 더 쉽다. 자체평가를 하여 상급경영진에 방책에 대하여 통보하거나 제출하는것이 더욱 성과적일것이다. 자체평가는 여러가지 방법으로 진행할수 있다. 그러나 효과적인 방법은 방책을 믿음직한 보안원칙과 비교하는것이다.

중요한것은 방책작성자가 기관에 방책들이 작성되여 있는가 하는것을 확인하는것이다. 방책들이 작성되여 있다면 그것들을 하나로 련결시킬 새로운 방책을 작성해야 한다. 이미 있는 형식으로 새로운 방책을 작성하면 기관성원들은 새로 작성된 방책을 쉽게 리해할것이다. 그러나 이렇게 이미 있는 형식으로 방책을 작성하지 않으면 사람들은 작성한 새 방책을 방책으로 보지 못하게 된다.

건의되는 방책형식은 아래의 체계로 되여야 한다.

- **배경** 왜 방책이 존재하는가.
- **범위** 방책은 누구에게 영향을 주는가 그리고 방책은 어디에 필요한가.
- **정의** 용어들에 대한 해석
- **참고** 사람들은 어디서 보충정보를 찾을수 있는가.
- **조정자/방책작성자** 누가 방책을 주관하였는가 그리고 의문이 있으면 어디에 가서 질문해야 하는가.
- **위임관** 누가 방책을 위임하였는가.
- **효력날자** 언제 방책이 효력을 내는가.

- **재검토날자** 언제 방책이 재검토되는가.
- **방책사항들** 무엇을 해야 하는가.
- **례외조항들** 례외조항들은 어떻게 처리하는가.
- **제재** 위반행위를 알아 냈을 때 경영진은 어떤 대책을 적용할수 있는가.

기관들에서는 실정에 맞는 형식으로 방책들을 설계작성한다. 이런 경우에 방책문서에는 주요제목들과 화제들이 설정된다. 이 부분의 내용들은 이 장의 뒤부분에서 《공통형식의 설정》이라는 제목을 달고 제시한다.

표준의 규정

표준은 과업을 수행하고 그 성과를 평가하기 위한 규칙들이 어떤것들인가를 규정한다는것을 상기하라. 실례로 전기접속구의 모양이 어떻게 되여야 하며 국가적으로 어떻게 제작되여야 한다는것을 규정하는 표준이 있다. 제작자들이 표준을 지키면 그 접속구들을 팔수 있게 될것이다. 구매자들이 접속구들을 사면 그들의 설비는 그 접속구에 맞을것이다.

표준은 정기적으로 확인받아 그것을 준수하도록 해야 하기때문에 표준에 대한 설명은 간단하지 않은것이다. 전기접속구의 실례를 생각하자. 제작흐름선이 변화되여 완성된 제품에 영향을 주게 된다면 그 공정이 표준에 따라 평가될 때까지 구매자들은 그 접속구를 사용할수 없게 되여 결국 더는 팔수 없게 되고 비용이 많이 들게 되며 경영에서 혼란을 가져 오게 된다.

따라서 새로운 표준규격을 내오면 그 실현과 유지에 많은 비용이 드는것으로 하여 특별한 경우를 제외하고는 실제상 표준규격을 새로 만드는 기관이 좀처럼 없는것이다.

건의된 표준문서형식에는 아래와 같은 체계들이 포함된다.

- **배경** 왜 표준이 존재하는가.
- **범위** 누가 표준을 요구하며 그것이 어디에 필요한가.
- **정의** 용어해석
- **참고** 사람들은 어디에서 보충정보를 찾아 볼수 있는가.
- **조정자/표준제작자** 누가 표준을 주관하였는가 그리고 질문이 있으면 어디에 가서 질문해야 하는가.
- **위임관** 누가 표준을 위임하였는가.
- **효력날자** 언제 표준이 효력을 내는가.
- **재검토날자** 언제 표준이 재검토되는가.
- **표준사항들** 측정값과 요구사항들은 어떤것인가.

기관들에서 그에 알맞는 방식으로 표준들을 설계작성할수 있는데 이 형식은 방책의 문서안에서 주요제목들과 화제내용들을 설정한다.

표준을 완성하는것이 중요하지만 높은 실현유지비로 하여 흔히 그 수명 즉 재검토날자는 적어도 앞으로 5년은 되여야 한다는것을 강조하는것이 중요하다.

절차의 규정

절차는 기관마다 다르다. 절차작성에 대한 일치한 견해는 없다. 이전에 개발된 표준이나 대상청중에게 무엇이 가장 잘 작용하겠는가에 대한 시험에 기초하여 기관의 절차가 어떻게 되여야 한다는것을 결정하게 된다. 절차의 작성은 거기에 포함되는 세부지표들로 하여 가장 어려운 문제라고 말할수 있다.

절차의 작성은 거기에 포함되는 매우 높은 수준의 세부지표들로 하여 해당한 문서작성에서보다 보통 더 많은 인원을 요구하게 된다. 그러므로 절차개발을 담당한 책임자는 절차작성에 포함되는 단계들을 문서화하기 위하여 현재 그 일을 수행하고 있는 사람들과 같은 전문가집단을 구성하여야 한다. 이 문서화에는 주어 지게 될 실제적인 지령사항들, 이 지령사항들에 대한 론거들과 예견되는 결과들이 포함되여야 한다.

또한 절차를 작성할 때 쓰일수 있는 몇가지 형식들이 있다. 다른 문서들은 사람들을 특정한 방식으로 행동하게 하려는 경영진의 희망을 전달하기 위하여 작성되지만 절차에는 실제적으로 작업을 시키는 방법이 기술된다. 작성자는 이야기형식, 흐름도형식과 연극대본형식중에서 어느 하나를 선택할수 있다.

이야기형식은 문답형식으로 정보를 제공한다. 정보제공은 이야기식으로 무난히 진행되지만 사용자에게 리해하기 쉽게 단계적으로 진행되지는 못한다. 흐름도형식에서는 그림형식으로 정보를 제공한다. 이 형식에서 작성자는 론리적단계로 정보를 제공할수 있게 된다. 아마도 다른 방법들보다 더 많이 사용되는 연극대본형식에서는 사용자가 리해할수 있도록 지령사항들을 하나하나 제시한다.

대상청중이 알아 들을수 있는 수준의 언어로 절차를 서술하여야 한다는것을 잊지 말아야 한다. 이 장에서 토론되는 중요한 절차요소들은 절차의 필요성을 식별하는것, 대상청중을 결정하는것, 절차의 범위를 수립하는것과 절차의 취지를 기술하는 것이다.

건의된 절차문서형식은 아래의 체계로 구성된다.

- **배경** 왜 절차가 존재하며 절차와 관계되는 방책 및 표준문서들은 어떤것들인가.
- **범위** 누가 절차를 요구하며 어디에 그것이 요구되는가.
- **정의** 용어해석
- **참고** 사람들이 보충정보를 어디에서 찾을수 있는가.

- **조정자/절차작성자** 누가 절차를 주관하였는가 그리고 의문사항이 있으면 어디에 가서 질문을 해야 하는가.
- **효력날자** 언제 절차가 효력을 내는가.
- **재검토날자** 언제 표준이 재검토되는가.
- **절차사항** 측정값과 요구들은 어떤것인가.

기관들에서는 실정에 맞는 형식으로 절차들을 설계작성할수 있지만 이 절차형식에는 주요체계들과 화제들만 제시하고 있다.

지침의 규정

지침들은 바로 그 특성으로 하여 작성집행하기가 보다 쉽다. 지침은 경영진이 바라는 종업원들의 행동에 관한 법적구속력이 없는 건의안들이다. 종업원들이 자기 책임을 어떻게 수행하여야 한다는것을 기술하는 다른 문서들과는 달리 여기서는 종업원들이 마음에 드는 지침들을 택할수 있는 자유를 가진다. 어느 지침이건 그 준수는 전적으로 선택에 달려 있다.

방책작성자들은 지침들을 방책의 전 과정의 일환으로 작성한다. 그것은 문서들에는 강제력이 동원될수 없는 장려하여야 할 도의적문제들이 포함되여 있기때문이다. 이런 도의적문제들이 지침들의 기초를 이룬다.

다른 문서들과 마찬가지로 건의된 지침문서형식은 아래의 체계로 이루어 진다.

- **배경** 왜 지침이 존재하며 그것과 관련된 방책 및 표준문서들은 어떤것들인가.
- **범위** 누가 지침들을 요구하며 어디에 그것들이 필요한가.
- **정의** 용어의 해석
- **참고** 사람들이 어디에서 보충정보를 찾아 볼수 있는가.
- **조정자/지침작성자** 누가 지침을 주관하였는가 그리고 의문사항이 있으면 어디에 가서 질문하여야 하는가.
- **효력날자** 언제 표준지침들이 효력을 내는가.
- **재검토날자** 언제 표준지침을 재검토하는가.
- **지침사항** 지침내용과 요구사항들은 어떤것들인가.

다른 문서들과는 달리 지침승인자가 필요 없다. 지침은 대체로 큰 포괄범위로 작성되며 법적구속력을 가지지 않기때문에 승인서명이 요구되지 않는다.

방책의 발표

문서가 완성되면 기관의 종업원들 즉 성원들에게 보급되여야 한다. 이것은 종업원방책지도서, 부서소책자 그리고 직결전자출판으로 실현된다. 어떤 방책의 성과도 종업원들이 그 방책에 대하여 얼마나 알고 있는가에 좌우된다. 이것은 종업원들이 방책을 알아야 한다는것을 의미한다. 이를 위하여 기관에서는 종업원들에게 방책을 보급하며 종업원들이 앞으로 있게 될 방책의 변화를 알고 있도록 하는 방법을 가져야 한다.

방책지도서

각 기관들에서는 방책지도서를 잘 만들어 매 개인들에게 한부씩 보장하군 한다. 방책들을 참고하고저 하는 사람들에게 즉시적으로 보장할수 있는것으로 하여 이 사업은 일정한 기간 효과성이 높다고 한다. 그러나 지도서의 갱신과 같은 문제들이 제기되면 종업원들은 지도서들이 갱신될것을 기대하였다. 그러나 다른 긴급한 문제들로 하여 지도서들을 추세에 따라세울수 없었다. 그러므로 방책에 대한 검토문제가 제기되면 혼란에 빠지게 되군 하였다.

설상가상으로 기관들에서는 기관의 모든 성원들에게 문서를 공급하는데 드는 많은 비용은 그들의 리윤곡선에 부정적결과를 가져 온다는것을 리해하기 시작하였다. 기관들에서는 지도서비용으로 하여 종업원들이 창조하는 가치가 점점 줄어 든다는것을 깨닫기 시작하였다. 따라서 기관들에서는 전자출판을 방책보급에 리용하기 시작하였다.

부서소책자

모든 방책이 다 기관전체성원들을 위한것은 아니다. 기관산하의 개별적부서들은 또한 자기부서에 필요한 방책을 작성해야 하였다. 부서용 방책지도서작성이 가능하기는 하였지만 비용의 견지에서는 실용성이 없었다. 그러므로 부서들에서는 자기 분야에만 관계되는 방책들을 주는 소책자들을 만들었다.

방책의 직결배포

개인용콤퓨터의 증가와 정보에 대한 직결접근가능성이 커짐에 따라 더 많은 기관들에서 방책을 망에서 보급하게 되였다. 이런 사정으로 종업원들에게 새 방책과 새 자료들을 보급하는데서 높은 속도가 가능하게 되였다.

Web이 통신매체로 출현하게 되면서 기관들에서는 그것을 방책을 보급하는 수단으로 리용하고 있다. 하이퍼링크를 리용하여 기관들에서는 련관된 다른 문서들 및 참고자료와 련계를 맺어 줄수 있다.

의식화

그러나 종업원들에게 정보와 방책을 보급하는데 리용되는 매체에는 관계없이 종업원들은 자기들에게 필요한 방책들을 제때에 접수하는것이 중요하다는데 대하여 알아야 한다. 그리고 지어 매체도 심중하게 선택하여야 한다. 전체 종업원들이 콤퓨터를 다 가지고 있지 못하는 경우에는 또한 방책을 인쇄하여 보급하여야 한다. 끊임없는 의식화사업을 진행하여야 회사방책과 그것이 종업원들에게 주는 영향에 대한 종업원들의 인식수준이 유지될것이다.

공통형식의 설정

공통형식은 독자들이 방책과 방책보조문서들의 목적을 쉽게 리해하도록 한다. 이미 작성한 방책과 관계되는 문서들이 없는 경우에는 공통형식의 작성이 간단하게 된다. 기관안에서 쓰는 형식이 이미 있는 경우에는 공통형식의 작성이 더 힘들어진다. 그러나 작성자는 이미 쓰이고 있는 지면사용형식에 맞추어 문서들의 지면사용형식을 설정하는것이 중요하다. 이렇게 할 때 독자는 문서의 용도를 깨닫게 되고 기관에서 승인하는 문서의 내용을 리해하게 된다. 각이한 부분의 형식과 순서는 이 장의 앞에서 이미 제시되였다. 그러나 여기서 아래와 같이 간명하게 다시 제시한다:

- **배경**(모두)
- **범위**(모두)
- **정의**(모두)
- **참고자료**(모두)
- **조정자/문서작성자**(모두)
- **위임자**(방책, 표준, 절차)
- **효력날자**(모두)
- **검토날자**(모두)
- **처리**(모두)
- **문서사항**(모두)
- **례외조항**(방책)
- **제재사항**(방책)

달리 지적되지 않는한 이 부분들은 다 문서에 반영되여야 한다. 여러 문서의 구성요소로가 아니라 한 문서의 구성요소로 인정될수 있는 부분들이 있다. 일관성을 유지하기 위하여 이런 부분들을 모든 문서들에서 순서대로 제시하는것이 좋다.

이제부터 쓰게 되는 《문서》라는 용어는 방책, 표준, 절차, 지침을 의미하게 된다

배경. 무엇이 문서작성을 추동하였는가에 대한 정보를 제공하는 사항을 문서에 포함시키는것이 중요하다. 새로운 방책의 경우에는 일반적으로 특정한 사건에 대한 반응으로서 새로운 방책이 작성되기때문에 경영진의 결심을 추동한 내용을 문서에 포함시킨다. 다른 문서들은 새로운 방책을 참고할수 있게 그리고 새로운 방책을 지원할수 있게 작성하는것이 필요하다. 정황의 배경을 문서에 반영하여 독자에게 참고할 기준들을 제공한다.

범위. 어떤 정황들에서는 회사전체의 리익을 위하여 문서를 작성한다. 그러나 다른 문서들은 보다 적은 규모의 성원들에게 적용된다. 범위는 그 문서가 어디에 적용될수 있는가 하는것을 규정한다. 그리하여 사람들로 하여금 방책이 그들에게 적용될수 있겠는가 하는것을 결정할수 있도록 한다.

정의. 문서는 절차를 제외하고는 될수록 기술적은어가 없어야 한다. 절차외의 문서에서는 기술적은어가 독자들을 혼란시키는 경향이 있다. 그러나 일정한 정황에서는 이 용어사용을 막을수 없다. 그러므로 문서에 이 용어에 대한 해석과 정의를 잘 주어야 한다.

참고자료. 개발되는 문서에 중요한 참고자료를 제공하는 다른 방책, 표준, 절차 및 지침들을 포함하는 다른 회사문서들이 포함되여야 한다. 이 문서들은 이 방책과 이 방책을 지원하거나 혹은 이 방책이 지원하는 다른 련관된 문서들사이에 련관을 지어 준다.

Web상에서 출판을 위한 HTML파일로서의 문서를 작성하는 경우에 다른 련관된 문서작성에 하이퍼링크들을 포함시키는것이 좋을것이다.

조정자/저자. 조정자 혹은 저자는 문서를 개발하고 그에 대한 승인을 요구하는 발기인이다. 발기인을 방책문서에서 밝혀 주어야 그 어떤 질문이나 우려사항이 있어도 그 발기인에게 물어 볼수 있게 된다. 그러나 방책작성은 집단이 하고 실행책임은 상급경영자가 하는 경우에는 실지작성자와 조정자가 다른 사람일수 있다.

위임자. 상급경영진이 방책의 실현에 대하여 최종적으로 책임지기때문에 상급경영진의 한 성원이 방책을 승인하는것이 중요하다. 흔히 책임 있는 상급집행리사가 해당부문에 대하여 책임지기도 한다. 실례로 정보총괄책임자(CIO)는 정보체계방책에 대한 책임을 지며 재정총괄책임자(CFO: Chief Financial Officer)는 재정방책에 대한 책임을 진다.

표준이 회사표준으로 규정되자면 해당한 상급경영자가 그 표준을 비준하여야 한다. 표준이 한 부서에서 리용되자면 그 부서의 부장이 그것을 비준한다. 절차는 흔히 부서에서만 쓰이므로 부장의 비준을 받게 된다. 지침은 회사에서 사용되지 않는 조건에서는 비준을 받을 필요가 없다. 그런 정황에서는 기능을 책임진 상급경영인이 그런것들을 비준해야 한다.

효력날자. 이 날자는 문서의 효력을 내는 날자이다. 방책을 개발할 때 방책을 지원하며 방책의 효력을 발생하기에 앞서 사용자교육에 충분한 시간을 돌리는것이 중요하다. 방책지원의 경우에도 사정은 마찬가지이다. 그것은 방책을 발표할 때 사람들이 문서에 접근하고저 하는 사정과 관련된다.

검토날자. 검토날자는 문서를 앞으로 언제 검토한다는것을 설정한다. 시간이 지

남에 따라 모든것이 변하기때문에 검토주기를 정해야 한다. 문서에서는 시간주기를 정하는 사항, 정황과 사건으로 하여 검토가 필요한 사항들을 명기하여야 한다. 검토날자를 정하여 문서가 정확하며 적당하다는것을 립증할수 있다.

처리. 기관안에서 일정한 형식으로 문서를 분류 및 통제하는 경우에 처리와 관련된 특정한 지시들이 이 부분에서 제시되게 된다. 특별한 지시가 없는 경우에는 그 부분을 삭제하거나 특별한 지시가 없다는 사항을 보충한다.

문서사항. 방책조항은 경영진의 의도가 무엇인가 하는것을 기술하는 몇개의 본문행들로 구성된다. 방책사항은 길지 않으며 한개 문단을 넘지 말아야 한다. 이보다 더 긴 경우에는 방책이 모호해 질수 있다. 방책조항들은 종업원들이 요구되는 행동이 어떤것인가를 알수 있도록 명백해야 한다.

표준조항들은 표준을 제시하는데 필요한 세부내용을 제공할수 있도록 충분히 길어야 한다. 이것은 표준이 어떤 경우에는 아주 길어 질수 있다는것을 의미한다. 절차조항들은 또한 집행하여야 할 정확한 명령과 수행해야 할 과업들을 제기하기때문에 아주 구체적이다. 또한 포함된 세부의 수준으로 하여 절차조항들은 아주 길어 질수 있다.

례외조항. 이 부분은 일반적으로 방책문서에만 포함된다. 례외조항들을 어떻게 다룰것인가에 대한 사항을 방책문서에 포함시키는것이 좋다. 가령 한가지 방법은 례외를 문서화하는 공정을 세우는것이다. 이때 례외가 정황을 다루는 가장 실천적인 방법으로 되는가에 대한 설명을 주게 된다. 이렇게 되면 해당한 담당자들이 식별되고 동의를 첨부하면 그 경영인들이 제외조항들을 비준하게 된다. 례외조항들은 특별한 수명을 가진다. 실례로 이런 조항들은 해마다 재검토된후에 수명이 연장되여야 한다.

위반조항과 제재조항. 이 부분은 흔히 방책문서들에 포함된다. 기관들에서는 흔히 제재효과를 위하여 방책조항의 명료성을 보장하지 않는것이 일반적인 경향이다. 적용할 제재를 결정할 때 경영진이 문제를 신축성 있게 대할수 있도록 제재조항들을 폭 넓게 설정하여야 한다. 실례로 기관에서는 사소한 위반행위로 하여 종업원을 해고하지 말아야 할것이다. 인사부서와 법무담당부서는 제기된 제재를 재검토하고 승인할 필요가 있다.

공통적인 개발공정의 리용

이 모든 법률문서작성에서는 공통적인 공정이 리용될수 있다. 문서들을 개별적 사람들이 작성하자면 많은 사람들이 망라되여야 하며 따라서 그들의 시간을 다른 계획들과 일치시켜야 하는 경우에 문서작성의 과정은 흔히 개발과제관리방법으로 운영된다. 그런 방법이 필요 없지만 개발과제관리방법과 병행하여 이 공정을 리용하면 경영진으로 하여금 문서작성을 잘 지원하게 할수 있다.

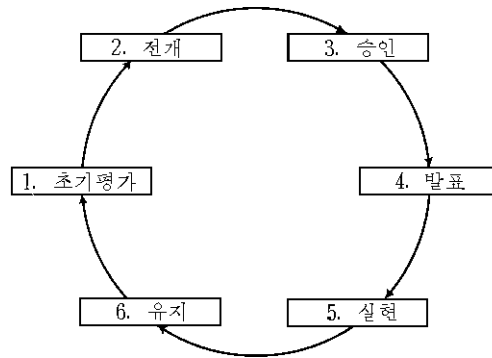



그림 20－2. 문서의 규정 및 개발

이 문서들을 규정하고 개발하는데서 리용할 공정의 한 실례는 그림 20－2에서 보는 바와 같이 여러개의 단계들로 이루어 진다. 이 매 개발단계는 다음 단계로 넘어 가기전에 완성되여야 할 별개의 과업들로 구성된다.

제1단계 : 초기 및 평가단계

특별한 문서(방책, 표준 등)의 필요성과 목적들을 서술한 서면제의가 경영진에 제출된다. 경영진은 지출비용과 기관리득을 정확히 계획할데 대한 이 요구를 만족스럽게 평가하게 된다. 이런 경우에 개발팀이 조직되여 제2단계에서 서술된바와 같이 문서를 전개하고 연구한다. 그렇지 않은 경우에는 사업을 더 추진시키지 말데 대한 권고가 문서제출자에게 떨어 지게 된다.

제2단계 : 전개단계

전개단계에서는 기관의 대상계획에 자금을 투자한다. 기관에서는 새로운 팀을 조직하든가 혹은 이전에 다른 대상계획에 참가한 팀을 그대로 인입할수 있다. 이 팀은 경영진과 함께 완성된 계획을 누가 비준하겠는가 하는것을 결정하여야 한다.

이 팀에는 리해관계를 가진 모든 당사자들과 필요한 능력을 소유한 사람들이 다 망라되여야 한다. 다시 말하여 이 팀에는 경영진의 대표, (필요한 경우에는) 계획실현을 책임진 운영부서, 개발팀, 기술전문필자와 최종적으로 봉사 및 제품접수자로 될 사용자집단의 한 성원이 망라된다.

경영진의 대표를 참가시켜 그들이 기관경영진의 나머지 성원들과 법률담당 및 기타 내부기관들과의 련락을 보장하게 할수 있다. 개발단체는 제품 또는 봉사개발공정이나 완성품조립공정에서 필요한 요구조건들에 필요사항들을 계속 추가한다. 운영부서 일군들은 문서가 일단 완성되면 실제적으로 실천단계에로 들어 가도록 조직사업을 한다. 개발단계에서는 사용자집단을 무시할수 없다. 문서의 조건을 접수할수 없는 경우에 사용자들은 자기들의 조건을 사전에 전면에 제기하여 개발과정을 단축할수 있다. 마지막으로 기술작

성자는 문서에서 쓰이는 언어를 창조하는데 방조를 준다. 대부분의 사람들은 그들이 언어를 잘 쓸수 있다고 생각한다. 기술전문필자들은 언어사용에 대한 전문교육을 받은 사람들이다. 이 팀의 성원들이 이런 역할을 자기들의 첫째가는 의무로 접수하지 않는다면 그들은 다 보조자로 된다는것을 알아 두라. 그들은 표준의 내용에 기여한 자기들의 지식에 따라 그리고 문서에 비준한 자기들의 이름과 더불어 인정 받는 전문지식에 따라 보수를 받는것이다.

이 팀은 개발과정의 심장이라고 할수 있다. 이 팀의 전문가들에 의하여 요구들이 제기되고 설계되며 언어로 표현된다. 이 사람들은 최종적인 언어표현에 대한 합의가 이루어 질 때까지 그 문제들을 토의검토한다. 만장일치는 좀처럼 어려운것이므로 다수가결로 문제를 결정하게 된다.

여러번 반복하여 초안이 개발되고 본래의 설계목적이 달성되면 그것을 기관의 많은 사람들이 검토평가하게 한다. 검토기간은 보통 30일이고 팀밖의 사람들로부터 의견을 반영해 넣게 된다.

이 검토기간에 문서는 모의실험에서 검토되여야 한다. 실례로 개발되고 있는 문서가 절차에 관한것이라면 경험이 많지 않은 사람도 절차사항에 기초하여 과업들을 성과적으로 수행할수 있어야 한다. 그들이 잘 수행할수 없는 경우에는 문서에 부족점이 생겨 그것을 퇴치해야만 비준을 받을수 있는것이다. 개발팀에서 문서를 검토하고 문서가 기술적으로 완성되였다고 하는 경우에는 제3단계로 넘긴다.

제3단계 : 비준단계

설계단계가 끝난 다음에는 기관안의 해당한 부서에 문서를 넘긴다. 일부 기관들에서는 방책비준방법을 일정한 형식으로 규정하지만 다른 기관들에서는 그렇게 하지 않는다. 개발단계에서는 비준단체 혹은 비준성원을 정할 필요가 있다.

문서를 비준부서에 제출한다. 거기서는 개발기간에 중요하게 고려해야 할 문제들을 강조하면서 개발공정에 대한 토론을 계속한다. 비준부서는 문서를 《비밀투표》로 결정하며 부정적인 문제들은 문서의 비준에 앞서 제기하여 해결하여야 한다.

제4단계 : 발표단계

마지막으로 필요하다면 문서를 번역하여 기관안에서 발표한다. 이때 문서는 효력발생날자에까지 이르러 실현준비가 다 된다. 어떤 정황에서는 실효날자가 발표날자로 될수 있다.

제5단계 : 실현

실현기간에 이 새로운 문서에 해당한 여러 그룹들은 그 문서를 실현하기 시작한다. 이 실현은 문서가 어디에 쓰이는가에 따라 각이하게 된다. 실례로 사용자의 견해는 운영부서집단의 견해와 다를수 있다. 문서가 사용될 때 사람들로 하여금 그에 대한 평가와

질문을 조정자에게 보내도록 하여야 한다. 이 평가들은 검토단계 또는 유지단계에서 중요한것으로 될것이다.

제6단계 : 유지단계

개발단계에서 결정된대로 문서를 검토날자에 검토한다. 이 검토기간에 문서의 지속적인 실행가능성이 결정된다. 실행성이 결정되여 변화시켜야 할 필요가 제기되는 경우에 그 팀은 제2단계의 개발주기를 가동시켜 그 주기를 다시 시작한다.

요 약

이 장에서는 정보보안에서 방책이 왜 중요한가 그리고 그 방책의 개발과 관련된 일부 문제점들과 분야들에 대하여 보았다. 정보보안방책은 기관의 지적재부나 다른 정보자산을 보호하기 위하여 경영진이 바라는것은 무엇인가를 밝힌다. 표준을 리용하여 공통적이며 접수되는 기준을 설정함으로써 모든 사람들이 그것을 리용하여 방책을 실현하게 한다. 절차는 세부들 즉 실현방법을 제공하며 지침은 경영진이 실현하고저 하는것을 밝혀준다.

방책은 해당 기관의 성원들이 어떻게 행동해야 하는가를 밝히기때문에 그 기관에서 필수적이며 중요한 한 부분으로 된다. 방책은 정보보안관리자에게 기관에서 중요한것은 무엇이며 그것을 위해 어떤 사업을 해야 하는가를 알려 준다.

참 고 문 헌

1. Peltier, Thomas, Information Security Policies, A Practitioner's Guide, Auerbach 1999.
2 . Kovacich, Gerald, Information Systems Security Officer's Guide, Butterworth–Heinemann 1998.

제21장. 신 뢰 문 제

레이 캐플린

최근에 보안과 관련된 바그에 대한 보도들이 소식통으로 계속 퍼지고 있다. 너무도 의견이 분분하여 핵심문제를 주시하기는 고사하고 지적하기도 어려운 형편이다. 무엇을 믿으며 왜 그것을 믿는가 하는 단순한 문제조차 종종 도외시된다.

더우기 기초시설들사이 및 기초시설내에서의 신뢰관계들의 필요성도 종종 스쳐보내고 있다. 신뢰와 그 중요성에 관한 핵심문제도 이따금 다 잊어버리군 한다. 보안은 신뢰문제이다. 이 장에서는 신뢰와 신뢰관계의 특성을 밝히고 신뢰를 리용하여 어떻게 안전한 하부구조를 축성하겠는가에 대하여 론의하게 된다.

신뢰문제란

신뢰는 보안에서 핵심문제이다. 그러나 안전한 하부구조를 구축해야 하는 경우에 신뢰에 대하여 단순히 리해하는것으로는 문제를 크게 해결할수 없다. 기관의 성원들, 기관과 그 성원의 고객들은 하부구조의 보안에 대하여 믿고 있다. 그런데 이상하지만 의존하지 말아야 한다. 사실 사람들은 계속 신뢰에 대하여 정확한 립장을 가지고 있지 못하며 흔히 잘못된 신뢰에 기초하고 있다.

이런 문제를 더 론하기에 앞서 신뢰란 무엇이며 신뢰를 리용하여 신뢰성 있는 하부구조를 어떻게 구축하고 유지하는가 하는것을 리해하는것이 중요하다.

신뢰의 정의

사전에서는 신뢰를 다른 사람 혹은 사물의 정직성, 무결성, 신뢰성, 공정성 등에 대한 확고한 믿음이나 신용이라고 각이하게 규정하고 있다. 사전에서는 또한 확실한 예상, 기대 혹은 희망, 안겨 주는 책임, 생겨 나는 확신에 대하여 서술하고 있다. 이것은 관계들의 발전을 념두에 두는것이다. 물건 또는 사람을 다른 사람이 돌보도록 맡기는것, 어떤 사람에게 어떤 일을 맡겨 주는것, 어떤 일이 일어 나도록 두려움없이 내 버려두는것, 누군가에게 신뢰를 허락하는것을 고려하라. 이 모든것들은 대부분의 사람들이 행동하는 방식(개인으로, 시민으로, 기관으로 그리고 사회적으로 또한 국부적으로, 전국적으로 그리고 세계적으로)에 대한 실례들이다.

인터네트, 법률, 전자상업거래, 언어학 등에 대한 신뢰의 실세계모형문제에는 아래의 한가지 기초정의가 적합하다.

> 신뢰는 통신통로에서 근본적인것이지만 그 통로를 리용하여 한 대상으로부터 다른 대상에로 전달될수는 없는것이다.

정보리론을 기초로 삼을수 있다.

> 정보리론에서 정보는 지식이나 의미와는 아무런 관계도 없다. 정보리론의 견지에서 정보는 통신통로를 리용하여 한 대상으로부터 다른 대상에로 전달되는것일따름이다.

신뢰를 정보에 첨부된 가치로 생각하라.

사람들이 보안문제와 관련하여 신뢰에 의거하게 되는 실례들은 콤퓨터사용과 망사용의 모든 경우에 있게 된다. 실례로 한 조작체계의 일정프로그람은 실행대상들을 제공해주는 장치에 대한 신뢰에 기초한다. TCP/IP망규약묶음은 파케트의 원천주소(보안장치가 원천신원의 립증을 요구하지 않는한)를 그 발신자로 볼수 있다고 확신한다. 대부분의 사용자들은 그들이 접근하는 열람기들과 Web싸이트들이 자동적으로 보안상 《정확한 일을 한다》고 믿는다. 이렇게 하여 사용자들은 그들이 의거하는 조작체계의 일정프로그람과 망규약묶음들을 믿는다. NSA는 신뢰 받는 체계 또는 구성요소가 보안방책을 파괴하는 힘을 가진것이라고 신뢰에 대하여 아주 잘 요약하고 있다. 그러나 대부분의 기관들은 신뢰에 대하여 이렇게 생각하지 않는다.

개발, 전개 및 리용되고 있는 (널려 있는)체계들의 보안에 관한 모든 문제들이 바로 신뢰에 달려 있기때문에 이 신뢰라는 모호한 문제를 푸는 방법을 아는것은 매우 중요하다. Windows NT와 Windows 2000과 같은 분산형신뢰모형들을 가지고 있는 조작체계들과 PKI를 실례로 보면 될것이다.

신뢰가 아닌것

신뢰가 아닌것에 대하여 토론해 보는것이 또한 중요하다. 신뢰에 관한 자기 글에서 E. Gerck박사는 매우 협소하게 정의된 어떤 실례들을 제외하고는 신뢰가 이동, 분포, 련합 혹은 대칭적인 특성들을 가지지 않는다고 설명하고 있다. Gerck는 간단한 실례들, 수학적인 증명들과 실세계경험을 들어 신뢰를 설명하고 있다. Gerck는 보안의 실천적경험을 중시하기때문에 《리론은 최종적으로 현실에 대한 부합성에 기초하여 평가되여야 한다》고 한 뽈스까수학자 스따니슬라브 레슈니엡스끼(Stanislaw Leshniewski)의 말을 인용하고 자기 글을 시작하였다.

신뢰에 관한 규칙들이 항상 무시되기때문에 유닉스체계들사이의 신뢰를 처리할 때, 공통적인 주요하부구조들과 분포된 하부구조들을 구축할 때 그리고 Microsoft Windows 2000의 새로운 보안모형의 실천적측면들을 다룰 때 사람들은 계속 마음이 좋지 않아 한다. 이것들이 문제성 있는 분야들의 몇가지라는것을 알아두라.

시작에 앞서 한가지 말해 둘것이 있다. 말하자는것은 Windows 2000의 품위를 떨구는 문제가 아니라 Windows 2000이 다음과 같은 문제들을 잘 보여 준다는것이다. 즉

- 신뢰규칙들이 어떻게 빨리 깨여 지는가.
- 신뢰모형을 평가하는 사업에 착수할 때 구체적인 세부문제들은 어떻게 되는가.
- 규칙들을 파괴하는 신뢰모형들이 제기하는 문제점들.

조사사업, 수학적인 증명들 그리고 실세계경험에 기초한 단순한 실례들을 들면서 다시 말하여 Windows 2000의 기초신뢰모형문제에 대한 개론으로부터 시작하여 Gerck박사의 주장의 하나인 이행성에 대하여 살펴 보자.

신뢰는 이행적인것이 아니다. X가 Y를 믿고 Y가 Z를 믿는다 하여도 X가 Z를 자동적으로 믿을수는 없다. 즉 내가 당신을 믿는다는 단순한 사실은 당신이 믿는 모든 사람들을 내가 믿게 되는 리유로는 되지 못한다. 이것은 PGP모형과 같은 《신뢰의 망》모형들의 주요한 제한요인이다. 신뢰관리문제들을 다루는 가까운 친구들 또는 동료들의 그룹을 위한 전자우편보안쏘프트웨어로 PGP가 개발되였기때문에 이것을 쉽게 리해할수 있는것이다. 신뢰성은 《닫긴 그룹》안에서 매 성원이 허락하는 정도의 이행성만을 띤다. 《닫긴 그룹》밖에서는 신뢰가 존재하지 않는다. 그룹의 규모가 크므로 《믿는》그룹성원이 제출하는 신임장들에 대한 신뢰를 그룹에서 제한하지 않을 때에는 문제가 일어 난다. 결과 체계들이 《관계되는》보증서들에 의거할 때에는 문제가 제기된다. Windows 2000이 그런 체계라는것은 이 체계가 이행성 있는 신뢰에 기초한 모형을 가지고 있기때문이다. 이행성 있는 신뢰가 Windows 2000체계에서 리용될수 있다고 기대하는것은 그 작용에 대한 아래의 설명에서 보는바와 같이 바로 문제성이 있는것이다.

첫째로, 《일차적인 신뢰령역》들을 언급하고 있는 《Windows NT봉사기표준》문서에서 인용한 문단은 Windows NT 4.0과 Windows 2000의 차이들을 제기한다.

> …신뢰령역은 국부체계가 사용자들을 인증하는 령역이다. 다시 말하여 사용자 혹은 응용프로그람이 신뢰 받는 령역에 의하여 인증되면 그 인증은 이 신뢰령역을 신뢰하는 모든 령역들에서 접수된다.

Windows NT 4.0체계상에서 신뢰관계들은 일방적인것이므로 명백하게 설정하여야 한다. 두방향신뢰가 명백하게 설정되면 두개의 단방향신뢰들이 이루어 진다. 이런 류형의 신뢰는 비이행적성격을 띠는것으로서 한 령역을 믿으면 그 령역이 믿는 다른 령역도 자동적으로 믿는다는것을 의미하지는 않는다.

> Windows NT 4.0워크스테이션에서 《신뢰령역》의 대상은 신뢰분야들보다 오히려 주요분야를 위한 정보를 인증하는데 리용된다.
>
> …Windows 2000체계에서 매개 새끼령역은 자동적으로 어미령역과 두방향신뢰관계를 가진다. 기정값상 이 신뢰는 이행성 있는것으로서 한 령역을 믿는다면 그 령역이 믿는 모든 령역들도 역시 믿게 된다는것을 의미한다.

둘째로, 《Microsoft NT봉사기표준》문서에서 발취한것은 다음과 같다.

> Windows 2000령역들은 함께 련결되여 두방향이행성 있는 신뢰관계들을 가지는 ADS(Active Directory Server)《나무》들을 이룰수 있다. 사용지도서신뢰관계들과 같은 정적인 《싸이트련결다리》들을 설정하여 주면 ADS《나무》들은 뿌리에서 함께 련결되여 일반디렉터리도해와 세계목록봉사기가 있는 《기업체》 혹은 《수림》으로 된다.

마지막으로 《Microsoft 2000상급봉사기문서》에서 발취한것:

> 한 수림의 모든 Windows 2000령역들은 이행성 있는 신뢰로 련결되므로 같은 수림의 Windows 2000령역들사이에 한방향신뢰들을 창조하는것은 불가능하다.
>
> …Windows 2000수림령역의 신뢰들모두가 한방향이동성 있는 신뢰들이다.

《Microsoft 2000상급봉사기문서》에는 수림의 모든 령역들이 그 수림의 뿌리령역을 믿으며 령역들사이의 신뢰통로들 모두가 이행성 있는것으로 정의되여 있다고 지적되여 있다. 이 모든것은 우리가 알고 있는것과 크게 대립된다는것 즉 신뢰는 어떤 협소하게 정의된 경우들을 제외하고는 언제나 이동성을 띤다는것을 알아 두라. 이런 이행성신뢰의 존에 대한 암시 그리고 그에 동반되는 기정행위가 큰 난관들을 조성한다는것만을 말해 둔다. 전형적인 실례인 인적자원(HR)담당부서의 령역을 보자. HR정보의 기밀성으로 하여 하부구조에 있는 다른 모든 령역과의 자동적이며 포괄적인 령역간신뢰관계가 적합하다는 것은 명백하지 않은것이다. 실례로 HR를 자기의 령역에로 분리시켜 다른 령역들의 HR망 행정관리자들이 남의 자원과 보호대상들(파일들과 같은)에 접근하지 못하게 할수도 있다.

부적당한 이행성신뢰의 다른 실례들도 많다. 이런 신뢰가 왜 문제로 되는가, 그것을 어떻게 다루어야 하는가 그리고 유닉스환경에서 그와 관련된 문제들에 관한 실례들은 유닉스망파일체계와 원격접속설비들에서의 이동성신뢰에 대한 Marcus Ranum의 설명에서 찾아 볼수 있다.

신뢰는 분배되는것이 아니다. W와 Y가 둘다 Z를 믿는 경우에 W는 자동적으로 그룹으로서의 Y와 Z가 하나의 그룹이라고 믿을수 없다. 당사자의 기관과 당사자의 가장 큰 경쟁자가 둘 다 인증국(CA)에서 인증서들을 받는다고 생각하라. 후에 그 경쟁자는 인증국을 통채로 사 들여 바로 당사자의 모든 정보에 접근하게 된다. 당사자의 가장 큰 경쟁자가 당사자의 인증서를 무효화시키지 않으며 당사자의 모든 정보에 접근할수 없다고 자동적으로 믿을수는 없다. 실천적으로는(실례로 당사자의 CA와의 계약이 침해되는 경우에) 그런 정황에 대하여 소송을 제기할수도 있다. 그러나 CA들과의 합의가 이런 우발적인 사고에 대비할수 없게 되였기때문에 이렇게 하기는 어려울것이다.

또한 오직 태도를 바꾸어 다음과 같이 할수 있을것이다.

- 위법행위를 하는 CA와 그가 발급하는 신임장을 더는 믿지 않는다.
- 현재는 효력이 없는 이 신임장들을 무효화시킨다.
- 실현할수 있는 신뢰관계를 가지고 있는 CA로부터 새로운 신임장들을 받는다.

신뢰는 교제되는것이 아니다. X는 특별한 목적으로 하여 Y 및 Z와 맺은 동료관계를 믿지만 자동적으로 Y와 Z를 개별적으로는 믿을수 없다.

한 그룹(아마도 어떤 특별한 목적으로 하여 이루어 진)을 믿는다고 하여 그것이 바로 그 그룹안의 성원들을 다 믿을수 있다는것을 의미하지는 않는다. 특별한 목적으로 하여 두 경쟁자사이에 이루어 진 동료관계를 믿는다고 생각해 보라. 그것은 동료관계와 관련된 문제에서조차 그들을 개별적으로 믿을수 있다는것을 결코 의미하지는 않는다.

신뢰는 대칭적인것이 아니다. X가 Y를 믿는다고 해서 Y가 X를 자동적으로 믿을수 있는것은 아니다.

즉 신뢰관계들은 자동적으로 2중방향 즉 쌍방향으로 되는것이 아니다. 신뢰는 유일방향 즉 비대칭적인것이다. 내가 당신을 믿는다고 하여 당신이 나를 자동적으로 믿을수는 없다.

앞에서 여러번 설명된바와 같이 믿는측은 믿음에서 일정한 제한점을 결정한다. 믿음이 이동, 분배, 교제 및 대칭의 특성을 띠는 유일한 경우는 일정한 형태의 《가벼운 신뢰》가 존재하게 되는 경우이다. 즉 믿는측이 그것을 허용하게 되는 특정한 경우이다.

신뢰성

신뢰가 그 무엇에 믿음을 준다는것을 의미한다면 신뢰성은 그 믿음이 잘 구축되였다는것을 의미한다. 무엇을 믿는다는것은 그것을 가치 있게 만든다는것은 아니다. 가치 있게 만든다는것은 신뢰업무의 횡재이다.

많은 체계들과 망들을 믿을수 있지만 신뢰성 있는것은 거의 없다. 단순한 실례를 들어 보면 이 문제를 풀수 있을것이다. 가령 도시에 있는 일터에서 멀리 떨어 져 사는데 대중교통수단이 거의 없거나 없다고 생각해 보자. 그러면 자동차로 일하려 가게 될것이다. 아무 지장도 받지 않고 자동차로 출퇴근을 아주 잘할수 있을것이라고 믿을수 있다. 그러나 무더운 여름날 한낮에 자동차를 타고 《죽음의 계곡》(캘리포니아주 남동부의 한 건조분지-역주)을 가로 질러 갈수 있을것이라고 믿지 못할수 있다. 도시구역에서는 공중전화실에서 전화를 걸어 방조를 받을수 있기때문에 고장이 나도 생명에 위협으로는 되지 않는다고 볼수 있다. 그러나 죽음의 계곡을 가로 질러 려행할 때에는 방조를 받기가 매우 어렵기때문에 고장이 나면 물이 없어 생명이 위험에 처하게 된다. 이리하여 승용차가 통근에는 신뢰성이 있지만 위험한 환경에서 오랜 려행을 하는데는 신뢰성이 없다는것이 확증되였다. 즉 도시구역안에서 통근을 목적으로 하여 교통용으로 리용할 때에는 자기의 차를 믿게 된다.

쉽게 말하여 신뢰는 정황에 의존된다. 즉 사람들은 일정한 구체적인 정황에서 어떤것을 믿을 결심을 하게 된다. 신뢰는 믿음에 관한것이다.

사람들은 보안의 의미에서 자기 일을 정확하게 수행해야 할 때 체계들과 망들을 신뢰성이 있는것으로 볼수 있다. 즉 사람들은 특정한 조건에서 체계들과 망들을 믿게 된다. 결국 이런 믿음은 넓은 범위의 신뢰성에 이르게 된다. 이 범위의 한 끝에는 수학적증명에 기초한 이 주장에 대한 공식적인 확신을 요구하는 믿음 받는 체계들이 있다. 다른 끝에는 《그 체계는 자기일을 하고 있다》라고 말하는것 같은 오랜 기간에 걸쳐 수집된 증언자료들이 있다.

사람들은 신뢰(신뢰성)를 여러개 식으로 측정할수 있는 량으로 정의하려고 시도한다. 보안의 기술적측면에서 신뢰를 정의하려는 다음과 같은 여러가지 방법들이 있다. 즉

- 신뢰콤퓨터보안평가기준(또한 《오렌지책》으로 알려 진 TCSEC)과 이것을 계승

한 공통기준 및 그에 따르는 공식검수방법들과 같은 공식적인 기준들

- 방화벽검수실과 같은 상업제품시험실에서 진행되는 덜 공식적인 검수
- 공격에 견디여 낼수 있다는것을 보여 줌으로써 신뢰성이 있다는것을 증명하려고 하는 이른바 《도전싸이트들》
- 알려 진 모든 취약성들을 철저하게 알아 낼것을 목적으로 하는 침투시험
- 순수 기술적수단으로 찾을수 있는것을 찾아 취약성들이 있는 곳을 밝히는 평가
- 제품생산의 마지막공정이 끝나기전에 부족점을 식별하는 쏘프트웨어와 하드웨어의 알파판본, 베타판본 및 출하전판본

이 모든것들은 일정한 조건에서 체계 혹은 망들을 우리가 믿을수 있다는것을 보여주기 위한것이다. 이 모든것의 목적은 신뢰와 믿음을 구축하여 신뢰의 수준에 이르는것이다. 다시 말하여 체계와 망들이 신뢰성을 띠게 되는 조건을 구축하는것이다. 실례로 TCSEC의 오렌지책을포함하고 있는 이른바 레인버우총서에 있는 많은 자료들가운데는 신뢰체계의 전개방법을 서술한 《신뢰설비사용지도서작성지침》과 《신뢰설비관리리해안내서》가 있다. 지도서의 한 대목은 다음과 같다.

> 신뢰설비지침에는 체계들의 신뢰설비관리기능들을 문서화하는것과 관련된 훌륭한 관례들이 제시되여 있다.

《신뢰설비관리》는 안전체계구성, 관리 및 운영을 위하여 리용되는 행정경영절차, 역할, 기능(즉 명령, 프로그람, 대면부들), 특권들과 자료기지들로 정의된다.

체계가 안전하다고 믿지만 말고 체계가 전개되는 설비를 믿음직하게 관리하여야 한다. 군대식사고를 나무라지 말고 상업체계나 경로기와 같은 망구성부분들을 각성 있게 관리하여야 한다는것을 알아 두라.

이런 리론들과 여러가지 시험방법들은 제한성이 있다. 그러므로 언제나 실천에 적용되지는 못한다. 그러나 일반적으로 기준에 의거하면 신뢰성평가시험에서 높은 성적을 얻게 된다.

신뢰를 보장하는 문제에 대한 또 한가지 견해는 위험요소들을 가능한껏 제거하며 나머지는 그대로 두는것이다. 체계와 망들을 포함하여 위험요소가 없는것은 없다. 위험요소들을 가능한껏 없애고 나머지를 그대로 두게 되는것은 모든 위험요소들을 다 제거하자면 비용이 너무 많이 들기때문이다. 모든 위험요소들을 설사 다 제거할수 있다고 하더라도 보통 그 모든 위험요소들을 절대적으로 다 식별할수는 없는것이다.

신뢰가 왜 중요한가

신뢰와 신뢰성이 왜 중요한가 하는것을 리해하기는 쉽다. 필자가 찾은 전반적견해를 표현하는 가장 좋은 방법은 Francis Fukuyama가 쓴 책 《신뢰, 사회적미덕 및 번영의 창조》에 있다. 아래에 인용한 말은 생활에서 우리가 하는 모든것에 그리고 보안을 비롯한 콤퓨터 및 망작업에서 우리가 하는 모든것에 적합한것 같다.

나라의 복리와 그 실현능력은 유일하게 지배적인 문화적특성 즉 해당 사회에 고유한 신뢰수준에 의하여 제약된다.

기업체들의 복리와 그 실현능력은 그 하부구조들의 유일하게 지배적인 특성과 그것들이 의거하고 있는 특성 즉 고유한 믿음의 수준에 의하여 제약된다. 사람들이 자기의 하부구조를 믿지 않는다면 기대하던 모든것을 잃게 된다는것을 알아 둘 필요가 있다. 탁상형콤퓨터를 생각해 보라. 그것을 믿을수 없다 하더라도 그것을 리용하면 얼마나 편리하겠는가.

1990년 철학박사학위신청자로서 David Cheriton박사는 다음과 같이 평가하였다.

분산형체계들의 제한성은 그 성능에 있는것이 아니라 신뢰에 있다.

Cheriton의 말은 빵구이기계를 비롯한 모든 대상이 콤퓨터와 필요한 망장치를 가지고 있어 생활에서 외부의 모든 대상과 련결되여 있는 오늘의 시대에 잘 적용되는 말이다.

Robert Morris의 다음의 인용문은 이 착잡해 지는 복잡성의 호상접속의 현 실태를 아주 명백히 설명하여 주고 있다. 즉

대충 짐작해 보아도 서로 접속되여 있지 않은것이란 없다.

이것은 정말 믿기 어려운것이다. 사람들은 자기들이 어떤 사람들이라는것, 자기들이 가지고 있는것 그리고 자기들이 알고 있는것들을 믿을수 있는 근거는 고사하고 알지도 못하는 상대들에게 나날이 더욱더 의탁하고 있는것이다. 신뢰는 점점 더 중요한것으로 되고 있다. 그러나 대부분의 개별적사람들과 기관들은 재부를 잃어 버리거나 양도하게 되는 경우에야 신뢰를 리해하고 고맙게 여기게 된다.

왜 사람들이 신뢰하는가

앞에서 론의되였지만 사람들이 신뢰하게 되는데는 많은 근거가 있다. 대부분의 사람들이 신뢰성의 그 어떤 근거도 중시해야 된다는데 대하여 리해하지 못한다는것을 알 필요가 있다. 우리들중의 대부분은 믿게 되는데 그것은 눈먼 믿음이다. 근거는 아래와 같은것일수 있다.

- 《일은 제대로 되고 있다》라고 믿을수 있는 근거
- 반대의 증거가 없는것
- 공동체의 다른 사람들로부터 받게 되는 부분적인 증거

더우기 세계의 서로 다른 문화를 가진 사람들의 특성은 우선 신뢰하고 다음에 의문되는것이 있으면 질문하는것이다. 이것은 흔히 그렇지 않은 경우가 있기때문에 혼란을 주게 된다. 그러나 그것은 각이한 문화들에서 중요한 특성으로 된다.

왜 사람들이 믿지 말아야 하는가

신뢰의 중요성을 보여 주는 가장 중요한 방법은 아마도 불신 즉 신뢰, 믿음 혹은 확신의 결핍과 의심 혹은 의혹에 대하여 이야기하는것이다.

놀라운것은 사람들이 접수하는것의 대부분은 그들로서는 힘에 부치는것이라는것이다. 실례를 들어서 그 문제의 한 측면 즉 복잡성을 고찰하라. Marcus Ranum은 복잡성에 대하여 깊이 생각하면서 Web열람기들자체가 복잡성을 처리하기 위한 도구들로 되였다고 말하고 있다. 대부분의 열람기들이 지원하는 (HTTP, FTP, Telnet 등과 같은) 무수한 규약들을 처리해야 하는 복잡성을 숨기는 일을 대부분의 열람기들이 맡고 있다는것을 생각해 볼 필요가 있다. 우리들중 얼마나 많은 사람들이 계속 불쑥불쑥 나타나는 새로운 최신Web응용들의 모든 특징들과 매력들에 대하여 알고 있는지 Ranum은 묻는다. 아마도 그것을 아는 사람은 그것을 코드화하는 사람이라고 그는 말한다. 더우기 그런 규약보안의 세부는 발표되지 않았으며 판본마다 다르다. 여기에 활력을 주는 실례로서 Netscape열람기 4.06판에 나타난 《Smart Browsing》특징에 대한 이런 내용을 생각해 보라.

> Netscape Communicator회사가 내놓은 Communicator 4.06은 사용자가 지금 보고 있는 문서와 관련이 있는 싸이트들을 건의하는 봉사의 전단인 《관련내용》이라는 표시가 달린 새로운 아이콘에 의하여 조종되는 새로운 특징인 《Smart Browsing》을 포함하고 있다. 이 특성을 실현하자면 사적비밀과 관련된 수많은 잠재적인 우려들이 생기게 된다. 이런 문제들을 여기서 조사하였다.
>
> 특히 사용자가 Web을 탐색하는동안에 방문하는 URL들은 Netscape의 봉사기에 기록된다. 이 자료기록들은 쿠키와 접속되여 사용될 때 지어 이름, 주소 그리고 일부 경우에는 전화번호까지 포함하여 개별적인 Web사용자들의 확장서류를 구축하는데 리용될수 있다.

이 문제에서 난관에 봉착하는 경우에는 PKI와 Windows 2000과 관련된 신뢰문제들을 다 다쳐 보려고 하면서 더욱더 골머리를 앓을수 있다. Windows 2000으로 오래 쓸수 있는 신뢰모형을 구축하고 유지하기 위한 방도문제는 Windows 2000자체에 대한 신뢰방도탐구문제와 비교해 보면 아무것도 아니라는것을 알아야 한다. Windows 2000이 2,700만 혹은 4,000만의 코드행을 가지고 있기때문에 그 절반 또는 그이상이 초기출하판에서는 없다고 한다. 보안과 관련된 바그를 퇴치한 수자는 아주 놀랍다.

복잡성과 규약문제들이 이렇다 해도 대부분의 사람들과 기관들은 자기들의 하부구조들을 믿어야 할 리유는 없는것이다. 하부구조들을 믿지 못하게 되는것은 지역문제와 관련된다. 신뢰성이 있는 하부구조들은 거의 없다.

우리가 매일 겪게 되는 고의적인 기만에 대하여 생각해 보게 하는 문제들이 계속 제기된다. 이런것들에는 비루스, 웜 및 트로이목마들, 우리에게 밀려 드는 Bugtraq와 같은 일상보안설교와 공격자들의 적의가 속한다. 약삭빠른 경쟁자들은 기업이나 전쟁에서 있을수 있는 모든 기회를 다 리용하여 사람들을 속여 넘기려 한다. 《손자병법》을 참고자료로 건의한다. 기업경쟁자들이건 하부구조공격자들이건 적수들은 온갖 기회에 대상을

기만할것이라고 보아 진다.

하부구조를 믿을수 있는 근거는 무엇인가. 이에 대해서는 대체로 오직 한가지 답변이 있을뿐이다. 즉 우리는 그런 질문을 고려하지 못하였다. 그러나 하부구조를 믿을 근거를 찾지 못하고 있다. 어떤 사람들(그리고 모든 기관들)은 자기들을 기만하고 있다.

하부구조의 보안

이 문제의 본질을 보자. 물어 보아야 할 질문이 한가지 남았다. 《여기로부터는 어디로 가야 하는가?》 이 질문이 어렵지 않다고 말하자는것은 아니다. 하지만 어떻게 자기의 하부구조를 믿겠는가 하는것을 리해하기는 쉬우며 또 직관적인것이다. 대답은 비교적 단도직입적이다. 즉

1. 신뢰를 얻는 문제를 위험관리의 련습으로 보라.
2. 계획을 세우라.
3. 그 계획을 실현하라.
4. 계획의 효과성을 평가하라.
5. 필요하면 그 계획을 수정하라.
6. 1단계로 돌아 가라.

이것은 성공할수 있는 확고한 방법이다. 다시 말하여 담보가 있는 방법이다. 지령들을 집행하는 사람의 통제밖에서 일어 날수 있는 모든 사고들(즉 회사가 기업을 못하는것)도 방지할수 있기때문에 필자가 경험한데 의하면 이 방법이 실패한적은 없었다. 그것은 이 방법이 바로 문제해결의 기본모형이기때문이다. 이 방법은 위험관리로부터 시작하여 구체적인 세부문제들을 해결할수 있게 한다.

위험관리초보

위험관리는 단순히 방정식을 푸는 하나의 련습문제풀이로 볼수 있다. 그림 21－1은 위험관리공정이 어떻게 작용하는가 하는것을 보여 주는 단순한 그림이다. 몇개의 정의들이 보안으로부터 시작하여 이 공정의 작용을 읽어 볼수 있게 할것이다. 사전 《American Heritage Dictionary》는 보안에 대하여 《위험에서 벗어 나기, 안전》이라고 정의를 주고 있다.

이것을 출발점으로 삼을 때 다음과 같은 첫 난관이 제기된다. 즉 콤퓨터하부구조에 대한 위험과 안전을 어떻게 정의하는가. 몇가지 용어부터 시작하자.

취약성, 위협, 위험 및 대응조치. 널리 통용되는 보안용어들을 리용하여 자체참고용목록을 작성할수 있다.

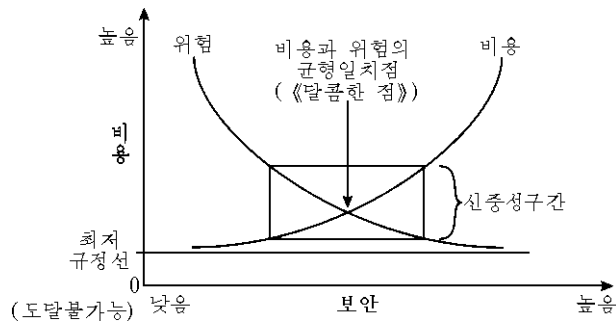



그림 21－1. 비용과 보안의 균형

- **취약성** 리용당할수 있는 약점. 다시 말하여 체계보안의 절차, 설계, 시행, 내부 통제조치 등에서 리용당하여 보안방책을 어기게 할수 있는 약점
- **위협** 취약성을 리용할수 있는 대상 혹은 사람. 다시 말하여 자료의 파괴, 개방, 수정 혹은 봉사거부의 형태로 체계에 손상을 입힐수 있는 잠재력을 가진 임의의 조건 혹은 사건
- **위험** 특별한 사건발생의 가능성 혹은 특별한 사건발생으로 입는 손실
- **대응조치** 특별한 취약성이 리용당할수 있는 가능성을 경감시키거나 특별한 취약성이 리용당하여 생길수 있는 파괴를 경감시키는 절차 혹은 수법. 다시 말하여 하부구조의 취약성을 경감시키는 기교, 행동, 장치 혹은 다른 조치(이 모든것들은 다 위험요소들이다)

이 방법은 존재하는 취약성들을 벌충하는 해당한 대응조치들을 적용함으로써 위험을 경감시키는데(단순히 조절하는데서가 아니라) 드는 비용을 위험을 당하는데서 보는 손실과 비교하는것이다.

이 방법에 대한 또 한가지 견해는 비용의 관점에서부터 문제를 대하는것이다. 그림 21－1에서는 비용과 위험의 호상관계를 보여 준다. 여기서는 또한 보안에 지출할 비용의 최적량을 어떻게 결정하겠는가 하는것을 보여 준다. 그림에서는 보안지출을 위하여 계산해 낼수 있는 최적량에 비한 보안의 실비용을 도해로 표시한다.

아마도 사람들은 일부 난관들에 봉착하게 되리라는것을 리해하기 시작할것이다. 공통적인 용어들을 제정하는것이 문제로 될수 있다. 어떻게 하면 이 용어들을 리용하여 하부구조보안과 관련된 복잡한 문제들을 잘 표현하겠는가 하는 생각으로 사람들은 공통용어들을 하나하나 골똘히 생각할수 있다.

아래의 세 개념들은 론리적으로 련관되여 있으며 토론을 위하여 하나로 묶어 놓을수 있다. 이 개념들을 리용하면 하부구조보안구축을 다음과 같은 세 단계로 간단히 표현할수 있다.

1. 취약성을 식별하라.
2. 취약성을 리용할수 있는 위협요소들을 식별하라.

3. 어떤 위협이 이 취약성을 리용할수 있다는 가능성을 경감시키기 위한 대응조치를 설계하고 실현하라.

이런 보안문제들은 매우 단순한것 같다. 그러나 대부분의 하부구조들은 너무나도 각이한 구성부분들로 이루어 져 있으므로 이 하부구조보안구축안을 실현하기가 어려운것이다. 그러나 이 안은 이 단계들을 반복하여 리용하는 반복공정이다. 리상적인 정황에서는 반복공정에서 매 기반구성부분들에 대응하는 위협, 취약성과 대응조치를 고려하게 된다. 경험에 의하면 하부구조의 매 구성부분들을 이런식으로 조사하지 않으면 하부구조의 보안을 보통 실현할수 없게 되는것이 일쑤이다.

그러나 실천적견지에서 말하면 이런 안은 가장 작은 기관들을 제외하고는 모든 기관들에서 실현할수 없는것이다. 이 보안구축공정을 거치는동안 기관의 기업을 중지한다고 생각해 보라. 결국 하부구조는 기관의 기업요구를 지원하기 위하여 있는것이지 결코 그 반대로는 되지 않는다.

이 규범에 대하여 유일하게 례외로 되는것은 훌륭한 보안이 설계의 목표이며 그에 따르는 자원담보가 있는 경우이다. 실례로 최신부분품이나 완전히 새로운 하부구조가 설치되고 있는 경우에 그런 기회가 불가피하게 있게 된다.

대부분의 사람들은 이런 보안은 군대에서나 실현할수 있는것이라고 믿는것 같다. 그러나 대부분의 경제분야들이 자기의 정보재부를 보호하는 문제에 큰 관심을 가지고 있으므로 보안에 대하여 심중하게 대하고 있다. 이런 대상들에는 대부분의 산업, 공업 및 교육기관들이 속한다.

기관의 기업을 멈추지 않으면서 이 위험관리실행을 어떻게 완성하겠는가 하는데 대한 실천적문제를 푸는 방법에 대하여 보자.

분석과 정량화. 취약성들을 찾아 내여 퇴치하는데서 기본은 분석과 정량화라고 말하여도 과언은 아니다. 이것은 거의 모든 경우에 대부분의 기관들이 기업적 혹은 기술공학적견지에서 보안을 대하지 않는 사정과 관련된다. 더우기 많은 기관들이 제기되는 문제들을 지어 확인해 보지도 않고 보안기술을 서둘러 사 들이려 하고 있다. 이런 생각은 함정에 빠지는것이라고 말하고 싶다.

상업적 및 기술적인 문제성들을 해결하는데 경험 있는 사람들은 오직 분석 및 정량방법에만 의거하는것이다. 제기된 문제의 구체적인 정형을 료해한 다음에는 그것을 분석하고 결함퇴치의 첫 단계로서 분석결과들을 정량화하여야 한다.

그러면 취약성, 위협 및 대응조치들을 어떻게 분석하고 정량화하겠는가. 정보체계들을 보안하는 규률을 잘 세우기전에는 이런 사업을 진행할수 없을것이다. 사실 이런 문제는 충분히 리해되는 문제이다. 필요한 도구들과 해당한 기술은 준비되여 있다. 그러나 어느 도구도 완성된것이 없다는것을 알아 두는것이 중요하다. 어떤 경우에나 아주 성공적인 방법들에서는 우리의 기본용어목록에 수록되여 있는 개념의 또 하나인 용어 《위험》을 사용하고 있다.

여기서부터 지어 일보라도 더 전진하기전에 조심이라는 말을 해 두는것이 적당할것이다.

위험을 정량화하는것은 힘든 문제이다. 사실 이 분야에서 적합한 방법들을 개발하려는

모든 시도들은 지난 수십년동안 완전히 실패하여 왔다. Donn Parker는 자기책 《콤퓨터범죄와의 싸움》(Fighting Computer Crime, 1998년판)에서 이런 실패들이 어떻게 생겨 났는가 하는것에 대하여 정확히 설명하고 있다. 임의의 측정척도를 리용하여 협소하게 규정된 분야에서 특정한 등급들을 정량화하는데서 성공할수도 있다. 그러나 이 등급들을 특히 매우 널리 분포된 현대의 큰 기관규모에서 임의의 동일한 척도를 리용하는 다른 등급들과 일치시키는것은 불가능하다는것을 경험은 보여 주고 있다.

우리는 정량적위험평가방법들을 리용할수 있다. 그러나 경험이 보여 주는바와 같이 많은 분야들에서 질적평가의 어떤 형태를 리용하기를 그만두게 될것이다. 일반적으로 보안프로그람의 평가를 생각하여 보라. 사람들은 보안프로그람이 해당기관을 위하여 자기 역할을 얼마나 잘 수행하는가에 대한 의견에 기초하여 평가하려고 할것이다. 틀림없이 이런 평가는 《한심한것》으로부터 《훌륭한것》에 이르기까지의 질적평가등급들을 필요로 하게 된다.

위험요소들의 처리. 위험요소가 있을수 있다는데 대하여 말할 때마다 사람들은 긴장해진다. 그것은 보안해야 할 체계들과 망들이 있기때문이다. 위험요소가 《있을수 있다》는데 대하여 당황해 할 필요는 없다. 위험요소들을 정량화하려는 시도들이 나타나고 있다. 특히 보안과 관련된 사업들을 지원할 예산을 세울것을 요구할 때 이런 시도들이 뚜렷해 진다. 경영진과 통계원들은 공론에 귀를 기울이지 않으며 기술자들과 기사들은 세부적인것들을 요구한다. 누구나 다 일할수 있는 구체적인 자료를 요구한다. 여기에 어려운 문제가 있다.

무거운 책임을 지고 있는 체계관리자 또는 망들은 많은 시간과 필요한 자료들을 받은 조건에서 보안문제들을 인증할수 있다. 발생가능성에 의하여 인증된 보안문제들의 효과를 정량화할 능력에 대하여 아직 론의하지 못하였다. 이 문제는 곧 론의하게 된다. 이에 앞서 위험요소들을 어떻게 분석하고 정량화하겠는가 하는 문제를 간단히 보자.

무엇보다먼저 문제에 대한 정확한 정의, 분석 및 정량화를 모색해야 한다. 또한 문제를 해결하는데서 경험이 있는 사람은 언제나 문제해결목표들에 대하여 문의한다. 문제해결목표들을 규정하는 좋은 방법은 예견하는 완성정도에 따라 목표들을 구분하는것이다. 즉

- **필요한것.** 필요한 요소들은 문제해결에 요구되는 근본요소들이다. 이 요소들은 근본적인것, 중요한것, 의무적인것 또는 전제적인것으로 볼수 있다.
- **충분한것.** 충분한 요소들은 해결해야 할 문제를 적합하고 충분하고 만족스럽고 또한 완전한것으로 되게 하여 해결할 문제를 완성시키는 보충적인 요소들이다.

상업기관, 산업기관 및 교육기관들의 보안경험이 보여 주는바와 같이 합리적인 보안해결책의 선택에서 기본은 필요한것과 충분한것을 배합하는 기업적 및 기술적예술에 있다. 보안분야에서 이런 방법이 과학적인것은 아니다. 그러나 높은 수준의 보안은 엄밀한 수학적증명과 변량을 극력 제한하는 철저한 규칙들을 적용할 때에만 실현된다. 그렇지만 돈을 벌자면 돈을 써야 하는것처럼 보안을 보장하자면 비용을 들여야 한다. 이런 대응조치들이 너무 비싸다고 하여 걸써 대한다면 필요한 대응조치들을 구태여 인증할 필요가 없다.

보안에 대한 지출은 《도로상태에 맞게 고무다이야를 만드는 경우》와 같다. 보안과 관련한 믿음직한 자료값은 거의 없다. 이런 사정으로 하여 하부구조구성부분들의 보안을

잘 조직하고 시험하는데 필요한 초과인원들의 작업주수에 대하여 체계관리자 또는 망관리자가 경영진에 정확하게 설명하려고 할 때 특별히 따분하게 된다. 경영진은 보고된 정보자료들이 기업에 가치가 있다는것을 흔히 정량화할수 있다. 그러나 체계관리자 또는 망관리자가 이 평가값들을 보안예산에 믿음직한 수자로 직접 반영하는 문제는 거의 불가능한것이다. 보안부문에 대한 오랜 경험을 가진 박식한 사람인 Bob Courtney의 다음의 말에서 좀 위안을 받게 된다. 즉

보호해야 할 가치만큼 보안에 지출하라.

문제는 가치가 얼마나 있는가 하는것을 결정하는것이다. 대답인즉 비용과 위험사이의 알맞는 균형을 보장하는것이다. 그림 21－1에서는 이 균형이 실천적으로 어떻게 이루어 지는가에 대하여 도해로 보여 주었다.

보는바와 같이 보안량과 그 비용(위험요소들 혹은 보안의 결핍)사이의 균형점을 《달콤한 점》(sweet spot)으로 정의한다. 달콤한 점의 울타리지역을 포함하는 《신중성구간》이라는 표시를 한 네모칸이 있다는것을 알아 두라. 이것은 보안량과 그 비용이 균형이 맞는 구간이다. 이것은 위험과 보안수준을 견지하기 위하여 지출되는 비용을 완전하게 균형잡는것이 불가능하지는 않다 하더라도 매우 어렵다는 사실에 기초하고 있다. 다시 말하여 위험요소들 혹은 큰 비용들에 대해서는 널리 통용되는 표준에 기초한 즉시적인 평가에 앞서 위험량에 대한 분석이 있게 된다.

실례로 모든 비루스들을 몽땅 잡아 내는 비루스스캐너는 살수 없다. 그러면 더 많은 위험이 있게 된다. 다른 한편 실행할수 있는것도 엄격히 제한하는 보수적인 방책밑에서 운영하는 경우도 있다. 그러면 비루스가 그러한 환경에서 퍼지는 길이 훨씬 더 적어지기때문에 그만큼 위험은 더 적다.

이에 대한 또 한가지 생각은 《신중성구간》이 위험요소들과 지출들이 《적당한》지역이라는것이다. 일반적으로 말하여 《달콤한 점》의 오른쪽 위험곡선에 있는 점들은 지나치게 지출한것이다(필요한것보다 더 많은 보안). 《달콤한 점》의 왼쪽위험곡선에 있는 점들은 너무 적게 지출한것이다(필요한것보다 적은 보안).

제한. 그림 21－1을 주의하여 따져 보면 그 어떤 곡선도 령으로 되지 않는다는것과 두개의 령이 있다는것을 알수 있다. 제한에 관한 두가지 중요한 점들은 다음과 같은것들을 말해 준다.

- 령점들을 정의하여야 한다. 절대적인 령위험을 가지는 하부구조들과 절대적인 령비용이 드는 보안은 존재하지 않으며 창조될수도 없다.
- 최대값을 정의하여야 한다. 가지는것만큼 지출할수 있다. 그러나 불안정한 하부구조들은 여전히 존재한다.

간단하게 생각하라. 일반적으로 적게 지출하면 많은 위험을 당한다. 비결은 접수될수 있는 위험수준을 식별하는것이다. 그리고 이 지역은 그림 21－1에서 신중성구간으로 표시된다. 이 모든것은 다음과 같은 질문을 제기한다. 어떤것이 적합한지 어떻게 아는가 그리고 존재하는 위험요소들을 어떻게 결정하는가. 오래동안 써 오는 한가지 방법을 보자.

자작도구. 그림 21－2는 그림 21－1의 X축(보안수준)에 여러가지 위험평가방법을 보

충한것이다. 이 위험평가기준들은 위험을 측정하는 대용척도들이다. 매 척도에는 이 수준의 위험을 경감시키는 비용이 널리 리용되는 응당한 관심기준에 의하여 어떻게 인정되는가 하는것을 암시하는 표시들이 속한다.

지출기준	지출없음	비용최소	비용과 위험의 균형	장래의 투자	자원랑비
위험도기준	최대위험	과도위험	최고허용 위험	최저허용 위험	위험없음 (도달 불가능)
완성도기준	적합치 않음	완전치 않음	필요함	충분함	지나침
실현방식기준	무계획적임	편의적임	응당히 관심함	고심함	마비됨

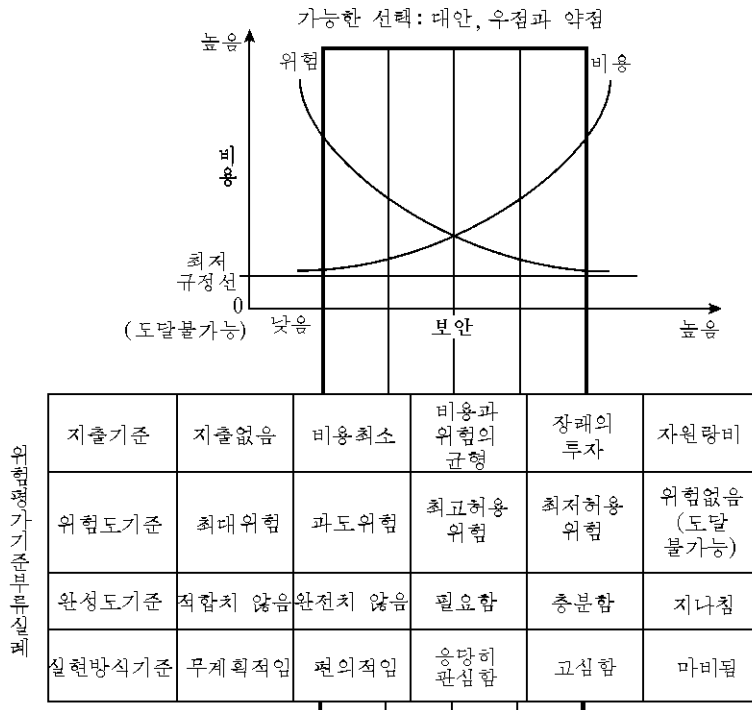



그림 21－2. 위험요소평가기준

X축(보안수준)아래의 보충정보는 명백한 표시들 즉 대안, 우점 및 약점이라는 표식들을 한 네모칸안에 있다는것을 알아 두라. 이 네모칸은 그림 21－1에서 임의의 지역이라는 표시를 한 네모칸(도해의 바닥에 수평으로 기록된)처럼 흔히 말하는 위험구간들을 둘러 싼다. 이 구간들(도해의 밑에 있는 개개의 위험구간들의 오른쪽옆에 기록된)은 각이한 위험요소평가기준에 의하여 결정된다.

실례로 지출기준의 위험요소평가기준들을 보라. 위험을 얼마나 허용할수 있겠는가 하는것을 평가해 보면 령지출과 자원랑비가 네모칸밖에 있다는것을 알수 있다. 령지출은 위험요소제거률이 너무 낮으며 자원랑비는 위험요소제거률이 너무 높다는것으로 볼수 있다. 이것은 바로 예견한 그대로이다. 실현방식기준의 위험평가기준들을 리용하면 명확한 선택들이 무계획적임(정량하기 쉬운것)으로부터 시작하여 응당히 관심함, 고심함에 이르기까지의 범위를 대안, 우점 및 약점이라는 네모칸이 둘러 싸고 있는것을 알수 있다. 그럴수밖에 없다.

선택하는 모든 기준들이 보충될수 있다. 이것들은 시작해야 할 실례들일뿐이다.

류의해야 할 문제:

위험요소들을 정량화하는 방법을 찾아 내려는 시도들은 대체로 실패하였으며 기껏해서

정량화방법을 찾았다 해도 적용하기 어려운것들이다. 이런 시도는 위험분석에 대한 정량적인 방법을 보장하려는 시도가 아닌것으로서 위험에 영향을 미치는 모든 요인들이 어떻게 호상작용하는가 하는것을 리해하는데 필요한것이 아니다. 사실 X축(보안수준)밑에 기록된 위험평가기준들이 실제적으로 량적측정값과 질적측정값들의 혼합이라는것을 알수 있다.

무엇이 중요하며 그것을 어떻게 측정할것인가 하는것을 물어 보는것은 가장 중요한 출발점이다. 질문을 제기한 이상 리용할수 있는 각이한 위험평가기준들을 고려해 볼수 있다. 연구해야 할 문제들이 많지만 그중에서도 가장 중요한 문제는 특정한 기관과 관련된 문제이다.

한 기관의 구체적실정에 맞는 응당한 관심, 일반적인 실천 및 규정준수의 표준들이 있다 .이 표준들은 산업분야의 고유한 측정값과 모든 기관들에서 공통적인 측정값의 관점에서 위험평가기준들로 리용될수 있는것들이다. 해당 산업에 대한 검열과 평가를 진행하여 온 검열관들과 전문가들은 한 기관에 중요한것으로 되는 해당 산업에 맞는 표준들을 제공할수 있으며 또한 흔히 응당한 관심과 일반실천이라고 보는것들을 제공할수 있다. 실례로 국방관련계약과 같은것을 담당한 산업부문들에서는 NT, UNIX, 경로기 등과 같은 특별한 체계들을 보호하기 위하여 보안산업이 할 문제와 관련한 폭 넓은 협정들을 리행해야 한다.

기관들에서는 또한 자기 기관의 경영방식과 문화에 맞는 위험평가기준들을 찾아 내야 한다. 물론 누구나 위험평가공식들과 그것을 집행하는 모형들 그리고 그림 21－2에 제시한대로 이 모든것을 자동적으로 수행하는 도구들을 찾고저 할것이다. 그러나 보안에서 지금 적용되는 분석과 정량화의 최첨단수준은 모든것을 마우스로 다 하는 방법과는 완전히 다르다. 마우스로 하는 방법들을 가지고서는 보안의 분석과 정량화문제를 다는 수행하지 못한다. 현재 사용되는 대부분의 도구들은 본질상 정교하게 작성된 계산표들이다. 그러나 이 도구들은 정량적인 위험평가방법들의 명목이나 유지할 정도로 방조를 준다.

현재 위험평가는 창조적능력과 경험이 있는 보안전문가들이 시끄럽고 하찮은 세부문제들을 하나씩하나씩 처리해야 할 문제를 많이 안고 있는 복잡한 문제이다.

결론적인 문제

복잡한것이 틀림 없지만 모든 기관들에서는 자기의 하부구조보안공정을 잘 파악하고 널리 실천해 나가고 있다. 비결은 계획을 가지고 기업의 관점에서 정보체계와 망하부구조들을 대하는데 있다. 수행할 단계들과 적용할 방책들이 있다. 다시 말하여 오래동안 검증된 하부구조보안을 처리하는 방도가 있다.

1. 하부구조들에서 보게 되는 취약성들과 위협들을 식별하라.
2. 취약성들과 위험성들을 성문화하라.
3. 기관의 기업상요구를 반영하여 위험요소들을 등급별로 구분하라.
4. 대응조치들을 식별하고 그 균형을 맞추라.
5. 위험요소목록을 작성하기 위하여 공격계획을 작성하는데 착수하라.
6. 가장 큰 위험요소들을 결합시키는 사업에 오늘 당장 착수하라.

신뢰구축

하부구조에 대한 신뢰구축사업이 사람들이 잘 리해하는 공정이라는것을 알면 독자들은 기뻐할것이다. 신뢰를 쌓는 문제를 문서로 만들어 널리 실시하고 있다. 사실 문서에는 실례들이 아주 많다. 신뢰구축에 대한 훌륭한 참고자료는 《주요기관들로부터 배우기》라는 책에 있다. 참고자료가 정부문서라고 하여 사람들이 무관심하지 않도록 하라. 그 자료는 주요사영부문과 정부기관에 의하여 훌륭하게 적용되는 공정에 기초한 좋은 참고자료이다. 필자는 이 모형의 개작판을 리용하여 보안평가를 하였다. 이 GAO모형은 확장되여 공정의 한 단계를 선행하는 일부 단계들을 포함하게 되였다. 이것은 실천에서 효력있는 기술의 일부로서 그림 21−3에 제시되였다.

그림 21−3을 살펴 보면 거기에는 반복되는 순환이 있다는것을 알게 된다. 모형의 평가단계는 위험평가에로 확장되였으며 그것을 안받침하는 부분들은 다음과 같다.

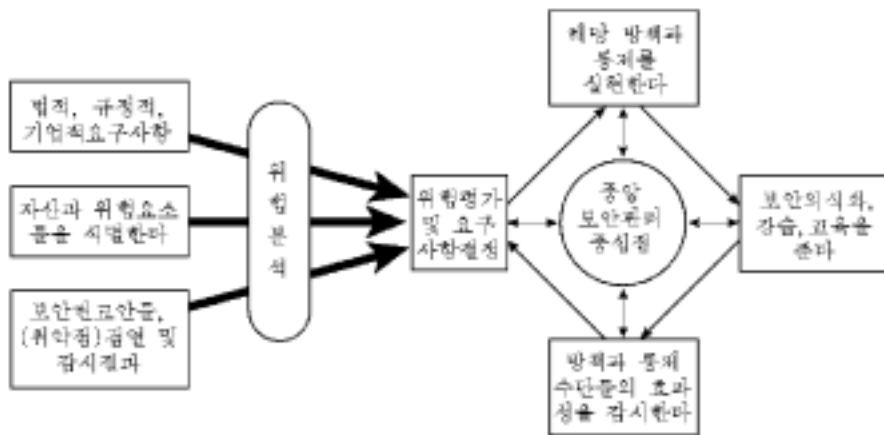



그림 21−3. 신뢰구축계획

- **법적, 규정적 및 기업적인 요구들** 기관의 의무집행자세를 식별하는 공정(즉 기관이 어떻게 일해야 하는가를 결정하는 법조항 및 감시조항)
- **자산 및 위험요소식별** 기관에서 더 중요한 부분들을 갈라 내고 그 부분들의 재부에 대한 위협들을 색출하는 공정
- **보안권고안들과 검열 및 감시결과들** 하부구조취약성식별공정

하부구조의 특정한 구성부분들에 대한 신뢰를 구축하면서 겪은 세부들은 또 하나의 연구론문에 담을만한 이야기이다(그림 21−3에 제시된바와 같이). GAO보고에 제시된것과 같은 모형대로 위험요소들을 식별하여 경감시키는것은 하부구조의 신뢰를 구축하는 확고하게 믿을수 있는 방법이다.

※ 될수록 많이 참고할수 있게 하려는 목적에서 참고문헌들에서 URL들도 주었다. Web의 불안전한 특성으로 하여 URL들은 때때로 변할수 있다. URL이 동작하지 않는 경

우에는 http://www.google.com과 같은 유능한 검색기구에 검색문자렬로서 참고자료제목을 주면 해당한 페지가 나타난다.

참 고 문 헌

1. Gerck, E., *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.htm.
2. Gerck, E., *Certification: Intrinsic, Extrinsic and Combined*, MCG, http://www.mcg.org.br/cie.htm.
3. Gerck, E., *Overview of Certification Systems: X.509, CA, PGP and SKIP* http://www.mcg.org.br/cert.htm#CPS; Gerck, E., e-mail message titled: Towards a Real-World Model of Trust, http://www.mcg.org.br/trustdef.txt; Gerck, E., e-mail message titled: Re: Trust Properties, http://www.mcg.org.br/trustprop.txt.
4. Leshniewski, Stanislaw, (1886–1939) http://www-groups.dcs.st-and.ac.uk/~history/Mathematicians/Leshniewski.html.
5. Gerck, E., taken together: E-mail message titled: *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.txt and e-mail message titled: Re: Trust Properties, E. Gerck, http://www.mcg.org.br/trustprop.txt; Gerck, E., *Summary of Current Technical Developments Near-Term Perspectives for Binarily-Secure Communications*, http://www.mcg.org.br/report98.htm.
6. *Primary and Trusted Domains, Local Security Authority Policy Management*, Microsoft MSDN Online Library, http://msdn.microsoft.com/library/default.asp?URL=/library/psdk/lsapol/lsapol_2837.htm.
7. *Microsoft Windows NT Server Standards*, http://www.unc.edu/~jasafir/nt-main.htm.
8. Taken together: Microsoft Windows 2000 Advanced Server Documentation, Understanding Domain Trusts, http://www.windows.com/windows2000/en/advanced/help/sag_AD_UnTrusts.htm — for the table of contents which contains this article see: http://www.windows.com/windows2000/en/advanced/help then choose *Security Overview* then choose *Trust*. Other references one can use to gain an understanding of how the new Windows 2000 trust model works include the following Microsoft online help document heading: *Understanding domain trees and forests*, http://www.windows.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_ADintro_16.htm. In addition, see *Planning Migration from Windows NT to Windows 2000*, http://www.microsoft.com/technet/win2000/win2ksrv/technote/migntw2k.asp.
9. Ranum, Marcus, *Internet Attacks*, http://pubweb.nfr.net/%7Emjr/pubs/attck/index.htm; specifically the section on transitive trust: http://pubweb.nfr.net/%7Emjr/pubs/attck/sld015.htm.
10. Gerck, E., e-mail message titled: *Towards a Real-World Model of Trust*, http://www.mcg.org.br/trustdef.txt.
11. Gerck, E., Summary of Current Technical Developments Near-Term Perspectives for Binarily-Secure Communications, http://www.mcg.org.br/report98.htm.
12. American Bar Association, Legal Infrastructure for Certification Authorities and Secure Electronic Commerce, 1996, http://www.abanet.org/scitech/ec/isc/dsgfree.html.
13. Gerck, E., Towards a Real-World Model of Trust, E. Gerck, http://www.mcg.org.br/trustdef.htm, also Gerck, E., in a 1998 e-mail message defining trust, http://www.sandelman.ottawa.on.ca/spki/html/1998/winter/msg00077.html which references the *American Bar Association Digital Signature Guidelines*, http://www.abanet.org/scitech/ec/isc/dsgfree.html.
14. National Computer Security Center, *Guidelines for Writing Trusted Facility Manuals*, NCSC-TG-016.
15. National Computer Security Center, *A Guide to Understanding Trusted Facility Management*, NCSC-TG-015.
16. Fukuyama, Francis, *Trust, The Social Virtues & the Creation of Prosperity*, ISBN 0-02-910976-0, The Free Press, New York, 1995.
17. From a presentation on security in distributed systems by David Cheriton in a Computer Science Department colloquium at the University of Arizona in the early 1990s.
18. A comment made by NSA computer security researcher Robert Morris, Sr. at a National Computer Security Conference in the early 1990s. He was explaining why he has to work so hard on such things as eliminating covert channels in order to protect the 1000 bit keys that could unleash a nuclear war. (He is the father of the Robert T. Morris, who was responsible for the 1988 Internet Worm.)

19. Ranum, Marcus, *The Network Police Blotter, Login:* (the newsletter of USENIX and SAGE), February 2000, Volume 25, Number 1, http://pubweb.nfr.net/%7Emjr/usenix/ranum_1.pdf.
20. *What's Related? Everything But Your Privacy,* Matt Curtin, http://www.interhack.net/pubs/whatsrelated/; and Curtin, Matt, *What'sRelated? Fallout,* http://www.interhack.net/pubs/whatsrelated/fallout/.
21. Variously reported to be in that range: The Long and Winding Windows NT Road, Business Week, http://www.businessweek.com/1999/99_08/b3617026.htm, Schwartz, Jeffrey, *Waiting for Windows 2000,* http://www.Internetwk.com/trends/trends041299.htm; Surveyer, Jacques and Serveyer, Nathan, Windows 2000: Same body, two faces, http://www.canadacomputes.com/v3/story/1,1017,1961,00.html; Michetti, Greg B., *Windows 2000 — Another Late System,* http://www.canoe.ca/TechNews9909/13_michetti.html.
22. The bugtraq forum on http://www.securityfocus.com.
23. Tsu, Sun, *On the Art of War, The Oldest Military Treatise in the World,* an easily accessible version, can be found at http://www.chinapage.com/sunzi-e.html.
24. *The Skeptic's Dictionary,* http://skepdic.com/.
25. Connie Brock.
26. Parker, Donn, *Fighting Computer Crime,* John Wiley & Sons, Inc., 1998, Chapter 11, Information Security Assessments, in particular. A summary of risk assessment failure begins on p. 277 of this chapter.
27. There are two styles of risk analysis: quantitative and qualitative. Dictionary definitions imply how they work: quantification — "to determine, express, or measure the quantity of," qualitative — "of, relating to, or involving quality or kind," *WWWebster WWW Dictionary,* http://www.m-w.com/. In his book *Fighting Computer Crime,* Donn Parker presents a complete tutorial on them and why quantitative methods have failed.
28. Parker, Donn, *Fighting Computer Crime,* John Wiley & Sons, Inc., 1998, Chapter 11, Information Security Assessments, in particular. A summary of risk assessment failure begins on p. 277 of this chapter.
29. U.S. General Accounting Office, *Executive Guide, Information Security Management, Learning From Leading Organizations,* GAO/AIMD-98-68, Information Security Management, http://www.gao.gov/special.pubs/pdf_sing.pdf.

제２２장. 위험관리와 분석

케빈 헨리

위험관리는 왜 문제로 제기되는가, 위험관리를 하는 목적은 어디에 있으며 위험관리를 하면 어떤 좋은점이 있는가. 오늘날 지나치게 확장된 사업환경에서 《위험관리와 분석》이라는 말은 사람들이 늘 쓰는 또 하나의 류행어로서 《행정관리형》인간들을 늘 바삐 돌아 가게 하며 《기술형》인간들로 하여금 자기 사업을 제대로 하지 못하게 하는 하나의 류행적인 경향으로 볼수 있다.

그러나 위험관리는 집중적이며 공고한 대응책과 계획작성전략의 기초로 리용되는 경우에는 회사에 커다란 리익과 자금절약을 가져다 주게 될것이다.

위험관리는 효률적인 업무의 초석이며 있을수 있는 사고에 명백한 목표를 가지고 미리 예방대책을 세우는데 큰 도움을 준다. 많은 회사들에서는 위험관리의 중요성을 인식하기 시작하였으며 위험총팔책임자(CRO: Chief Risk Officer)를 임명하고 있다. 위험관리가 회사내의 각 부서들의 주요 기능의 하나라는 인식도 자리잡히고 있다. 이렇게 많은 사람들의 노력과 그 결과를 잘 조정한다면 전체적인 씨나리오는 더욱 더 뚜렷해 질것이다. 위험관리를 자기 직능의 하나로 진행하는 그룹에는 보안(물리적보안, 정보체계보안) 그룹, 검열그룹, 비상대책계획그룹 등이 있다.

이 모든 분야들이 위험분석을 진행하기때문에 이 그룹들의 사업을 잘 조정하고 배합하는것이 중요하다. 그러자면 정보를 공유하여 방향과 사건대응을 교환해야 한다.

위험분석은 관찰, 지식, 평가 즉 예리한 안목과 재치 그리고 행운의 파학이다. 그러나 더 많이 알수록, 더 열심이 일할수록 성공률은 더 크다.

위험관리는 발견한 위험을 회사의 리익에 맞게 가장 좋은 방법으로 처리하는 기교이다.

위험을 수학공식으로 표현할수 있다.

위험=위협×취약성×자산

어떤 공통적인 실례를 리용하여 이 공식을 쉽게 기업환경에 적용할수 있다. 운동장에서 다른 아이에게 공부 끌나고 학교 정문밖에 나가서 때리겠다고 으르는 한 골목대장 아이의 실례에서 매 구성부분을 다음과 같이 나눌수 있다.

- 위협은 여기서는 매를 맞는것이므로 그 위협이 십중팔구는 일어 나리라고 본다. 그 경우 다른 일이 일어 나지 않는한 그 골목대장이 위협한 후에 때릴 가능성은 80%로 볼수 있다(대응책은 후에 설명).
- 취약성은 다른 아이의 약점이다. 이 아이가 물리적공격으로부터 자신을 잘 방어할수 없다는 사실은 그 아이가 공격을 당하는 경우 100% 피해 볼것이라는것을

의미한다.

- 자산값은 계산하기 쉽다. 새 샤쯔나 바지값은 70딸라가량 된다(싸우다가 코피 터지고 옷이 분명 째지고 더러워질것이기때문이다).

따라서 이 씨나리오의 총 위험은 :

위험=80%×100%$70.00
위험=$56.00

이 위험평가의 가치는 어디 있는가 하는 질문이 제기될수 있다. 이 평가를 리용하여 해당 대책안들을 선택하고 그 근거를 설명하여 예방적인 행동을 취할수 있을것이다. 대책안들로는 25딸라를 주고 경호원(방화벽)을 채용하고 그날은 학교에 가지 않으며(체계를 닫고 기업을 하지 않는것) 혹은 손해를 보상하기 위해 보험에 드는것 등이다. 이것들중 처음것은 약점이나 취약성을 강화하는것이라면 셋째것은 자산가치를 보호하는것이다. 예방적인 행동으로는 위험을 제거하는 방법들, 례하면 그 골목대장과 친하든가, 육체훈련을 하든가, 격술을 배우든가 아니면 이 도시에서 떠나 다른곳으로 이사가는 등의 방법들이 있을수 있다.

따라서 이 실례로부터 출발하여 위험관리와 관련한 정의를 다음과 같이 쉽게 내릴수 있다.

- 위험이란 영업에 영향을 주어 회사의 목적을 달성하지 못하게 하는 사건을 의미한다.
- 위협이란 회사가 자기의 영업에 영향을 주는 사고를 낼수 있는 가능성을 의미한다. 일부 전문가들은 위협을 긍정적으로도 부정적으로도 묘사한다. 따라서 위협이 언제나 부정적영향을 미친다고 보는것은 확실치 않다. 그러나 흔히 그렇게 해석되군 한다.
- 취약점이란 위협이 교묘하게 리용할수 있는 약한 점을 의미한다. 취약점은 하복부나 아킬레스건과 같아 다른 부분에는 든든한 철갑을 씌웠어도 공격이 개시되면 전체 체계나 전체 망이 열려 짐으로써 위태로운 처지에 빠지게 될수 있다. 그러나 위험을 일정하게 긍정적인 씨나리오로 될수 있다고 보면 《취약점》대신 《좋은 기회》 혹은 《관문》이라는 용어를 써야 한다. 이런 씨나리오에서 관건적문제는 제때에 그 좋은 기회를 포착하고 리용하여 위협이 최대의 리윤을 가져오게 해야 한다.
- 자산은 위험에 의하여 영향을 받는 요소이다. 우의 실례에서는 자산을 그 개인의 옷으로 보았다. 이것을 위험분석에 대한 대표적인 정량적해석이라고 볼수 있다. 정량적위험분석에서는 위험을 순수 수학적인 관점으로 보고 매 위험에 수값들을 주며 앞으로의 위험관리결정을 규제하는 지침으로 사용하

려 한다.

정량적위험분석

정량적위험분석은 여러가지 좋은 점이 있다. 정량적위험분석은 다소 직선적인 결과를 제공함으로써 계산에 기초한 보고서를 상급리사들에게 제출할수 있게 한다. 또한 상당히 간단하므로 쉽게 표본형식으로 분석을 할수 있다. 해당 부문의 전체 전문가들의 지원과 조언 그리고 보조연구사업의 도움을 받으면 초기경험이 매우 적어도 정량분석이라는 품이 많이 드는 일을 해나갈수 있을것이다. 위험분석수행의 일부 단계들은 후에 취급하도록 한다.

그러나 정량적위험분석의 약점들도 쉽게 찾아낼수 있다. 이 분석방법은 예산적측면이나 재정검사적측면에서도 일정한 의의가 있지만 사고의 영향을 받는 많은 다른 요소들은 다 무시한다. 우의 실례에서 그 골목대장에 의하여 입을수 있는 피해정도를 어떻게 알수 있단말인가. 대체로 외부적인 피해(옷, 긁히거나 멍드는것, 코피나오는것 등)만 예견하였지만 있을수 있는 피해는 훨씬 그이상으로 될수도 있다. 기업씨나리오를 실례로 보면 어떤 콤퓨터체계가 손상을 입겠는데 그 손실이 어느 정도로 되겠는지 누가 어떻게 알수 있단말인가. 콤퓨터범죄상습범이 체계에 뚫고 들어 와 어떤 범죄행위를 저지르려고 마음만 먹었다면 공격의 범위와 피해기간에 제한이 있겠는가. 무엇이 도난 혹은 복사되였는지, 어떤 트로이목마나 론리폭탄 혹은 비루스를 주입하였는지, 어느 비밀정보가 로출되였는지 또한 오늘과 같은 경쟁시대에 어느 비공개고객의 세부나 자료가 빠져나갔는지, 이 모든 요소들이 미지의것이므로 자산에 대한 피해액을 그 어떤 믿을만한 수자로 표시한다는것은 거의 불가능하다.

이 장은 최근에 출판된 거의 모든 책들과 마찬가지로 위험에 대하여 부정적인 관점으로 보고 있다. 반대로 위험을 긍정적인것으로 보아도 좋은 기회를 성과적으로 활용하여 리익이 얼마나 되겠는가를 알수가 없다. 래일에 대응하지 않고 오늘에 대응한다거나 혹은 기회를 다 놓쳐 자산(회사)이 지도적인 지위를 잃고 시장진출이 좌절된다면 자산에 미치는 영향은 얼마나 크겠는가. 전형적인 실례로는 아마 주권시장을 들수 있을것이다. 그 어떤 사람이나 회사가 리상적인 행동시간(위험을 억제하는 시간)을 안다면 상당히 좋은것이다. 그러나 하루나 한시간 있으면 결과는 파국적이다.

정량적위험분석에서 평가하기 힘든 일부 요소들로서는 종업원, 주주나 소유자, 고객, 관리기관, 공급자, 신용평가기관들에 미치는 영향들이다.

종업원의 견지에서 보면 공격이 성공하여 초래된 피해는 심각하나 알수 없다. 공격이 종업원들의 사기저락을 노렸다면 공격으로 하여 영문모르게 생산능률이 감소되며 기능공 및 숙련공보유문제가 제기되며 고객들에 대한 불성실한 반응, 로동행정에서의 기능저하나 충돌 등이 유발될수 있다. 또한 이것으로 하여 새 기능공모집이 억제될수 있다.

회사가 주주들이나 소유자들의 기대에 맞게 사업을 진행해 나가지 못하면 주주나 소유자들은 자기들이 투자한데 대하여 인차 후회하거나 흥미를 잃을수 있다. 사고들이 련이어 일어 나 회사가 자기 생산목표를 수행하지 못하면 투자나 리윤을 다른 회사에 돌리는것을 막을수 없게 된다. 아무리 리유를 말하고 설명한다 하여도 이렇게 자본이 이동하면 그 회사의 금융적지위는 크게 영향을 받게 된다.

고객들은 무슨 일에서나 성공을 가져 오는데서 관건적요인으로 된다. 가장 좋은 제품, 가장 좋은 판매계획도 지어는 가장 훌륭한 종업원들이 있어도 고객들을 끌어 고객을 많이 보유하지 못하면 다 쓸데 없다. 흔히 회사의 위력은 우수한 제품에 달려있다고들 한다. 그러나 그 회사가 제공하는 제품이나 봉사에 누구도 관심이 없으면 무슨 소용이 있겠는가. 우수한 제품을 가지고 있으면서도 신용문제로 《나쁘게 보도된》일이 있는 회사보다는 렬등한 제품을 가진 회사가 더 일이 잘 되는 경우도 있다. 부기계산체계가 불안전하여 회사가 망한다면 필생품질담보가 소용없게 된다.

기업을 감독하고 규칙을 지키게 하는 관리기관들은 대체로 사회적압력과 정치적영향력에 대하여 매우 약하다. 어떤 회사가 불안전하거나 취약성 있는 영업과정으로 하여 평판이 나쁘게 되였다면 사회적압력에 못이겨 정치인들과 관리기관들은 《자동적》인 반사작용을 일으켜 실지 그 회사에 《수갑을 채우게》 되며 회사는 새로운 통제사항, 절차, 보고서, 소송 등에 불필요한 자금을 지출하지 않으면 안되게 된다.

심각한 사고와 재난을 겪은 회사들이 찾은 가장 큰 교훈들중의 하나는 모든 중요 고객들과 공급자들과 련계를 신속히 맺어 그들에게 회사가 아직 존속능력이 있으며 영업공정이 현재 계속되고 있다는것을 재삼 확인해 주는것이다. 이것은 이러한 그룹들속에서 신뢰를 유지하는데서 필수적이다. 회사가 심각한 사고를 일으켰다면 공급자가 새로운 원료와 지원, 신용을 제공하기 꺼려하는 경우에는 그 회사는 절름발이로 되여 시장진출능력을 재건하기 힘들게 될것이다.

이 모든 그룹들에 이 사고가 영향을 줄수 있는것으로 하여 또 이 요인에 수값을 적용하여 계산하기 어려운것으로 하여 많은 전문가들은 순수 정량적위험분석은 가능성과 실천성이 부족하다고 주장하여 왔다.

정성적위험분석

정량적위험분석의 대안으로 되는것이 정성적위험분석이다. 정성적위험분석은 씨나리오에 기초하여 위험을 평가하여 해당 사건이 미칠수 있는 영향을 재는 공정이라고 볼수 있다.

정성적위험분석에 대하여 말한다면 있을수 있는 사고들에 대하여 개괄적으로 쓴 간단한 씨나리오들은 수없이 많으며 이 씨나리오들을 발전시켜 연구하면 이런 씨나리오가 발생하는 경우 회사의 어느 분야가 영향을 받으며 이 분야가 받는 손해의 범위는 어느 정도인가를 잘 알수 있게 된다. 이것은 해당 전문가들의 최상의 예측에 달려

있다.

정량분석에서 진행한것처럼 위험을 수값으로 해석하는것이 아니라 피해분야에 대한 위험수준을 측정하는 기준이 있다. 위험분석팀은 어떤 형태의 사고들이 일어 날수 있겠는가를 회사의 운영환경에 대한 최고의 지식에 기초하여 결정해야 할것이다. 이것은 전략계획작성그룹이 지역별시장전략에 따라 진행하는 금융모형화와 류사하다. 씨나리오를 개시하고 사건에 영향을 주는 변수들을 입력하는 방법으로 위험팀은 사건이 영향을 미치는 매 분야들을 찾아 내고 《큰 영향》, 《보통 영향》, 《작은 영향》과 같은 단순그라프 혹은 상징적 표식인 3, 2, 1, 0에 기초하여 그 그룹에 대한 영향을 결정할수도 있을것이다. 모든 영향받는 분야들을 찾아 내면 매 분야의 값들이 집계되여 해당씨나리오가 발생한 회사에 미치는 총적인 영향이나 위험을 예측할수 있다. 순수한 재정적고려를 내놓고라도 분석에서 고려되여야 할 분야들은 생산능률, 생산의욕, 신용도, 사회적압력, 앞으로의 전략적창의력에 미칠수 있는 영향이다.

정보체계에 대한 위험분석을 진행할 때마다 중요하게 고려해야 할것은 AIC 3요소(리용성, 무결성, 비밀성이라는 정보기술의 3대목표–역주)를 반드시 지키는것이다. 위험분석은 체계의 리용성이라는 요구조건을 반드시 고려해야 한다. 체계가 끊임없이 가동하는것이 기본인가 아니면 보수를 위해 중단시키겠는가 아니면 영업과정에 심각한 장애를 줌이 없이 체계고장으로 하여 간단히 가동중지시키겠는가. 체계와 관련된 자료와 공정조종, 접근조종 그리고 그 기초를 이루는 기초방책들의 무결성도 철저히 검토해보아야 한다.

아마 지난시기 비밀루설로 자료로출위험이라는 분야만큼 부정적인 영상을 많이 받은 분야는 없을것이다. 고객의 사적정보가 크게 요란히 침해되면 그것은 많은 회사들에 있어서 치명적인 사고라고 할만도 하다.

AIC 3요소와 위험분석사이의 관계를 잘 조사해낼수 있는 가장 좋은 방법의 하나는 콤퓨터전반통제검열을 모든 정보체계에 다 실시해 보는것이다. 콤퓨터전반통제검열을 위한 설문서실례를 표 22－1에 주었다. 이것은 인터네트상에서 구입할수 있는 여러가지 류사한 문건들에서 편집된 간단한 조사서이다. 이 조사(표 22－1을 볼것)를 잘하면 숙련, 고장점, 하드웨어 및 쏘프트웨어지원, 문건작성 등과 같은 분야의 약한 고리들을 찾아낼수 있다. 이 모든것들은 그 어떤 체계에 사고가 위험으로 실지 조성되였을 때 그 분석에서 매우 귀중하다.

그러나 정성적위험분석은 정량적위험분석에서와 마찬가지로 자체의 약점을 가지고 있다. 경영진에게는 이것이 너무 느슨하고 불명확하게 보이므로 대응책으로 되는것들을 구입하거나 새로운 방책과 통제를 실시해야 하겠다는 필요성이나 원가 대 리윤분석을 해야 되겠다는 결심을 가지리만큼 뚜렷이 안겨오지 않을것이다.

이러한 리유로 하여 지금 많은 회사들에서는 이 두가지 방법의 분석을 종합하여 실시한다. 회사들에서는 씨나리오계발식 정성적위험분석(그림 22－1을 볼것)을 적용하여 사고의 영향을 받는 모든 부문들을 찾아내여 정량적위험분석을 적용하여 사고에 대한 일정한 추산에 따라 대략적인 딸라수치를 위험영향 혹은 손실에 대입한다.

표 22-1　　　　　　　　콤퓨터의 일반통제지침질문서

목적

검열자가 부서에 있는 쏘프트웨어도구와 콤퓨터체계 혹은 하드웨어에 대한 체계 및 공정분석을 할 때 우리는 검열자가 검열과정에 이 질문서에 내용을 기입할것을 촉구합니다.

이것은 우리로 하여금 회사전반에서 현재사용중에 있는 체계들을 찾아 내고 더 잘 감시하게 할것이며 이 체계와 관련된 위험들도 분석평가하고 이 체계들을 앞으로의 검열계획에 포함시킬수 있을것이다.

협조해주어 감사합니다. 모르시는 문제가 있으면 알란이나 저와 련계를 취해주십시오.

체계이름과 략어 ____________________

앞으로 련계가질 주요사람 ____________________

체계사용분야 ____________________

초기면담에서 할 질문들:

체계기능에 대해 우리에게 설명해주십시오:____________________

이 체계가 어떤 가동환경(하드웨어)에서 가동합니까?____________________

이것이 개인쏘프트웨어입니까? 예_____아니_____누가 공급자입니까?____________________

MTS(통보문전송체계)가 원천코드를 한부 가지고 있습니까?　　예_____아니_____

어느 부서에 있습니까?____________________

원천코드에는 누가 변경권한을 가지고 있습니까?____________________

파일예비본뜨기가 밖에서 계획되고 보관됩니까?　　예_____아니_____

체계사용자명단과 그들의 특권사항을 받아
　보려면 어떻게 해야 합니까?____________________

쏘프트웨어와 하드웨어수리보수를 위한 계약이 있습니까?　　예_____아니_____

한부 사본을 얻을수 있습니까?　　예_____아니_____

임무분담관계

같은 사람이 보안과 프로그람작성을 같이 하거나
　자료입력도 할수 있습니까?　　예_____아니_____

입력/처리/출력의 무결성과 정확성

모든 입력자료가 정확히 들어가서 처리되였는가를 확인하는
　입력자료편집검열과 총체적통제방법이 있습니까?　　예_____아니_____

누가 사업과정을 감시하며 사업태만을 밝혀냅니까?____________________

누가 출력/보고자료사본을 받아 봅니까?____________________

권한관계

누가 체계에 대한 높은 급의 접근권한을 가지고 있습니까?____________________

보안—물리적보안과 설정

하드웨어와 자료입력말단장치들은 안전합니까?
누구나 거기에 접근할수 있습니까? 특히 높은급사용자
워크스테이션같은데 말입니다. 예______아니______

각종 표의 보유

체계와 관련한 그 어떤 표가 있습니까?
(실례로 세금표, 사원식별표 등) 예______아니______
누가 이 표를 수정할수 있습니까?______________________________

문서

전체체계와 과정이 문서화됩니까? 예______아니______
이 문건들은 어느 곳에 보관됩니까?______________________________

말단사용자 숙련

누가 사용자들을 훈련시킵니까?______________________________
누가 체계관리자들을 훈련시킵니까?______________________________
지식 있는 예비대리자가 있습니까?______________________________

체계의 재해수복계획

이 체계의 재해수복계획을 준비하여 회사비상관리부에
철해두었습니까? 예______아니______
입구/출구 의례를 써보시오.______________________________

기타 의견들

____
____
____

사명과 목적을 료해한다
정보보호 요구사항을 료해한다
위험환경을 감평한다
어떻게 할것인가 하는 대안을 결정한다
위험대응책을 결정한다
대응책을 실현한다

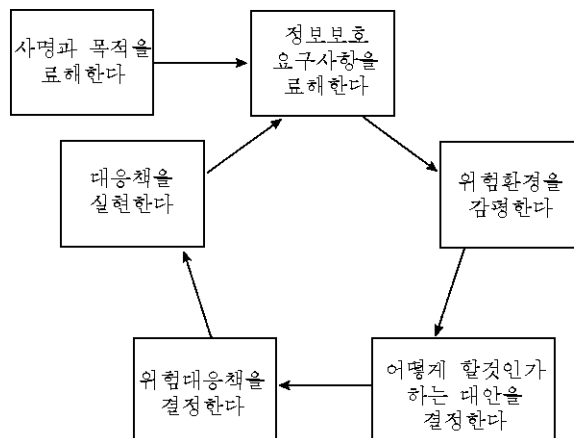



그림 22-1. 위험분석관리공정

물론 이것은 영업공정과 있을수 있는 위험에 대한 높은 수준의 료해와 지식을 전제조건으로 하고 있다.

관건적문제

위험분석에서 3가지 관건적요소라고 한다면 그것은 다름아닌 지식, 관찰, 기업가적안목일것이다.

지식

위험분석을 잘하려면 회사운영환경에 대한 철저하면서도 현실적인 료해가 필요하다. 위험관리자는 회사가 직면한 있을수 있는 위험요소들과 취약점들을 다 잘 알아야 한다. 새로운 위협형태, 경향성, 체계요소, 도구, 구조들에 대한 최신자료들을 다 알고 있어야 취약성들중에서 과장된것들과 지역적인것들을 갈라내고 자기기관에 적절한 대응책들을 강구할수 있다. 영업분야의 협조를 요청하여 위험분석을 진행하고 거기에서 얻어 지는 믿음직한 권고안들을 경영진에 제출하기 위해서는 위험관리자가 가능한 위협들과 대안들에 대한 현실적인 씨나리오를 제출할수 있어야 한다. 이러한 지식은 보안뷸레찐, 무역관계잡지, 검열기록들을 끊임없이 검토해 보는데서 얻어 지는것이다. 이렇기때문에 위험총괄책임자도 역시 고위경영진에 자리잡은 직무이므로 회사의 전략적방향을 알고 있으며 중요발기권을 가지게 되는것이다. 위험총괄책임자는 또한 회사에 영향을 줄수 있는 일체 사고정형을 수시로 보고받아야 한다.

관찰

관찰은 두번째 관건적인 요소이다. 우리는 자료범람과 통신범람의 시대에 살고 있다. 관찰이란 모든 외부의 영향들을 통찰하며 그 밑에 깔려 있는 씨나리오들을 리해할수 있는 능력과 기교를 말한다. 관찰에서는 모든 도구들과 보고서들을 수시로 검토하고 그 어떤 비정상적인 조건들이 있지 않는가를 알아 보아야 한다. 지적해야 할것은 많은 유용한 검사기록파일들 그리고 도구들이 제공하는 출력보고서들이 시간이 없고 힘들다는 구실로 한번도 들여 다 보지 않은채로 그냥 책장에 놓여 있다는것이다. 자기집 콤퓨터에 침입탐지체계(IDS)를 하나 설치한 후 처음으로 들여다 보면 자기 콤퓨터가 얼마나 많은 스캔을 당하고 공격을 받았는지 알고는 깜짝 놀랄것이다. IDS를 설치하니 스캔과 공격이 시작되였는가, 그렇지 않다. 정확한 도구를 구매하였으니 그 공격들을 관찰할수 있었던것이다.

따라서 관찰과 도구의 사용은 그 동작환경의 특성과 위험을 료해하는데서 필수적이다.

기업가적안목

위험분석의 기본리유는 결과를 얻자는것이다. 그러므로 세번째 관건요소는 기업가적

안목 즉 기업계에서 효과적으로 운영을 해나가는 능력, 방법과 기법을 감수하고 리해하고 사용하여 소여목적을 달성하는 상업가적재능이라고 할수 있다. 기업가적안목은 보통기업가와 능력있는 기업가를 가르는 척도이다. 기업가적재능이 있으면 일을 어떻게 솜씨있게 해내야 하는가, 설득력 있으며 신뢰성 있는 의견제시는 어떻게 해야 하는가, 《승냥이 온다》하고 소리치는식의 경고를 어느 때에 하고 언제 제꺽 빠져야 하는지를 잘 안다. 위험분석의 기초는 기업의 사명에 대한 리해와 달성이므로 위험관리자는 자기들의 전통적인 편견은 제쳐놓아야 하며 영업분야의 책임자들이 위험과 그 대응책을 분석할 때 그들의 립장에 서서 모든것을 리해할수 있는 능력을 반드시 가져야 한다.

위험관리대책안이 리상적으로 되자면 사용자, 영업분야책임자들과 능력 있는 행정일군들의 지원을 받아야 한다. 이것은 대책안이 사용자들에게 지나치게 간섭적이거나 시끄러운것으로 되지 말아야 하며 지원을 주는 영업체계나 영업공정에 생산능률이나 작업수행상 큰 영향을 주지 말아야 한다는것을 의미한다.

위 험 관 리

이제부터는 위험관리라는 과학이 효력을 나타내야 한다. 위험관리란 있을수 있는 사고들을 방지, 탐지, 수정하기 위하여 영업공정들과 체계에 통제를 실시하는것과 위험관리대책안이 기업의 정상흐름과 시간에 방해를 주지 않도록 하는 요구사항과의 적절한 균형을 말한다.

위험평가 및 분석이 완결되였으므로 그 결과는 회사에 주는 가능한 모든 위험들을 간단명료하게 개괄한것이여야 한다. 이 개괄보고서에는 발견된 모든 위협요소들, 매 위협요소들에 의하여 영향을 받을수 있는 부문, 로출(실행되는 위협요소)에 의한 피해액, 매 영업그룹에서 주요역할을 수행하는 사람 등이 목록으로 반영되여야 한다.

이 평가보고서를 보고 위험관리담당자는 해당 위험이 일정한 형태의 대응책을 취하는것을 필요로 하고 있는가를 평가해야 하는것이다. 흔히 이 대응책들은 세가지 부류 즉 약화, 할당, 접수로 나누어 질수 있다.

약화

위험을 약화시키기 위해서는 대체로 일정한 새로운 조종수단이 도입되여야 한다. 이 조종수단들로는 관리적(균형조절, 개인식별조종, 공정변화 혹은 물리적접근 규칙), 기술적(침입탐지체계, 방화벽, 구조구성, 새로운 도구도입)수단들이 있다.

위험범위와 기업운영요구사항들을 정확히 감정하고 평가하기 위하여 위험관리자는 위험들에 대한 가능한 대안들의 목록을 작성해야 할것이다. 이 대안들은 원가, 효률, 사용자리용의 견지에서 평가해 본 다음에 비준에 제기하여 실행시켜야 한다.

위험분석과 위험관리공정이 이쯤 이르고 보면 초기위험분석공정에서 느끼던 공포와 흥분은 점차 가라앉거나 사그라 들기 시작한다. 사람들은 새로운 문제들에 달라 붙게 되

며 몇주일전까지만해도 밤을 패가며 일하지 않으면 안되던 그 위협에 점차 무디여 지게 된다.

바로 이러한 시점들에서 많은 위험관리공정들이 탈선하기 시작한다. 대안들이 제기되고 지어 제품까지 들여 왔으나 그 실행의 추동력은 점점 맥이 빠져간다. 누구도 들여다 보고 그 특성을 모두 알려고 하지 않아 새로 들여 온 도구들도 도외시된채 놓여 있다. 통제가 약해지고 무력해진다.

예산지출이 되지 않아 통제에 대한 행정적지원이 계속되지 못한다. 이것은 보안관리자에게 있어 암흑의 나날로 될수 있다. 그 결과는 대개 불완전한 위험분석과 불완전한 위험관리공정으로 된다. 자, 이제 실행을 눈에 앞두고 그 계획은 조용히 사라져 간다.

이것은 위험관리자들에게 있어서 난관이 아닐수 없다. 위험관리자는 그 기회에 일떠서서 의식화계획을 작성하고 새로운 통제의 중요성을 설명하며 모든 사람들에게 자기 부서와 자기 회사의 앞날의 건강에서 이 위험대안이 얼마나 중요한 역할을 하는가에 대하여 알도록 하여야 한다.

외탁(Outsourcing)

오늘날 많은 회사들이 찾고 있는 하나의 대안은 위험관리도구의 채용과 위험관리의 할당사이의 결합수법이다. 이것은 위험관리공정의 주요분야들에서 외부의 자원에 위탁하는 개념이다. 정보체계의 보안을 위하여 일련의 도구와 제품들을 관리하는 유능하고 지식있는 일군들을 다 가지고 있다는것은 회사로서는 힘든 일이다. 따라서 여러 회사들에 위험관리봉사를 24시간 제공하는 유능하고 기능 높은 인원들을 가지고 있는 판매업체나 제조업체의 전문기술을 써 먹는수밖에 없다. 이렇게 되면 수많은 자체전문가들을 계속 전습을 주고 양성해야 하는 회사의 품을 덜어 줄뿐아니라 제3자의 독자적인 평가와 권고를 통하여 일정한 정도의 갱신조치를 취한다는것을 보여 줄수도 있다. 그러나 이것은 상당히 어려운 문제이다. 약속한 봉사가 제때에 제공되지 않을수도 있으며 제3자에게 맡겨진 기업망에 대한 정보와 내용이 안전하고 비밀에 붙여 지도록 회사는 노력해야 한다. 여우를 데려다 닭장을 지키게 하는것보다 더 어리석은 일은 없을것이다. 외탁협정을 통하여 위험총괄책임자는 해당 지원회사사업의 성실성을 평가할수 있는 권한을 보유하도록 하여야 한다.

할당

위험을 할당한다는것은 위험의 일부를 다른 회사에 맡기거나 넘기는것을 말한다. 이것은 일종의 보험계약이나 봉사계약을 통하여 실현된다. 보험자들도 회사의 위험에 대하여 상당히 철저한 검열을 요구하여 모든 위험들이 다 통지되였는가, 옳바른 작업과정이 실행되고 있는가를 확인해 본다. 이러한 보험도 구체적으로 평가하여 봄으로써 사고가 발생하는 경우 보험자의 보상이 어느 정도의 제한성이 있는가를 리해하도록 하여야 한다.

가능한 일부 보험분야는 봉사거부, 전자상업거래의 중절, Web싸이트의 손상들에 대한 보험이다.

접수

위험이 그리 큰 정도가 아니거나 대책안을 통하여 허용수준으로 약화되였을 경우 잠재적위험에 대한 접수가 필요하다.

일정한 수준의 위험을 접수하기 위하여 경영진은 그 위험범위를 결정하기 위한 위험분석공정을 평가해 주어야 한다. 경영진에 이 결과자료가 제출되면 경영진은 위험접수에 서명해야 한다. 이것은 위험이 약한 정도이므로 그 영향으로 인한 비용보다 대응책비용이 더 많이 든다는것 혹은 위험예방책이 현재 없으므로 할수없이 그 위험은 허용해 두지 않으면 안된다는것을 의미한다.

요 약

위험분석과 위험관리는 격동적으로 장성하는 분야이다. 한 회사가 위험을 찾아 내고 사고나 로출을 미리 막을수 있는 능력을 가지고 있다는것은 끊임없이 증가되는 위험요소들과 곤난속에서도 기업의 지속적인 존속과 성장을 담보하는 하나의 중요한 리익이다. 기업의 요구에 맞게 자기들의 노력을 조정하며 새로운 사태발전과 새로운 기술에 발맞추어 나가는 능력을 가지고 있다면 그것은 곧 뛰여난 위험관리자와 세속적이며 무능한 위험관리자를 가르는 척도로 된다.

위험관리와 위험분석에 대한 보다 깊은 연구를 하려면 주소 http://WWW.iatf.net의 Information Assurance Technical Framework(IATF: 정보보증기술체계)를 참고하기를 바란다.

제２３장. 정보위험관리의 새로운 추세

브레트 레간

최근년간 회사들이 정보보안에 대한 투자를 늘이고 있는것은 이전과는 달리 기간업무체계들이 점점 더 큰 위협을 받게 되는것과 관련되여 있다. 전자자료교환(EDI)체계, 전자자금전달(EFT)체계, 원격접근, 판매의 자동화와 같은 새로운 기술을 받아 들임으로 하여 기밀자료들이 있는 곳들이 점점 더 큰 위협을 받게 되였다. 인터네트를 리용하는 현상은 최근의 현상으로서 위험을 가장 많이 받는 분야로 되고 있다. 그러나 앞을 내다 보는 회사들은 인터네트상에서 위협요소들의 급속한 증가에 아랑곳하지 않고 맞받아 나아가 경쟁력을 높이는데 매진하고 있다.

정보위험관리는 새로운 분야로서 일반적인 전자정보체계를 뒤따르고 있다. 오늘까지 대부분의 기관들에서 정보위험관리는 주로 《풋내기》적방법으로 진행되여 왔다. 대개 전문가들의 의견을 받아 현안보호의 필요성에 대한 도움이나 받았지 앞으로 생길 위협들은 어찌할 생각도 못하는 실정이다. 전자적인 요새화사업도 기관들이 방어태세를 개선하는데 목적이 있었다. 이러한 대책들은 기업들로 하여금 통제와 위협이라는 정교한 균형을 가지고 기업운영을 하게 하면서도 지금까지 보면 일정하게나마 성과를 거두었다. 그렇다고 하여 그 기관들이 콤퓨터범죄의 타격을 받지 않았다고 말하는것은 아니다. 이러한 범죄들이 그 규모와 회수에 있어서 상당이 낮은 수준에 있었으므로 정보보안부서들과 보안팀들이 정보위험관리를 충분히 잘하고 있는듯한 인상을 주었을런지도 모른다.

전통적수법

기성위험분석은 하나의 잘 정립된 학문으로서 기업들의 결심채택에 도움을 준다. 위험분석은 무질서한 우연적인 사건들을 정돈하는데 가장 많이 리용된다. 발생가능성빈도률이 굉장히 높은 어떤 사건의 빈도수를 관찰하면 그 무엇이 언제 어떤 정도로 발생하겠는가를 일정한 정확도로 추측해 낼수 있다. 이렇게 하면 앞으로 100년동안에 7급의 지진이 10번이나 요꼬하마시에 일어 날것이라는것도 예측할수 있다. 매 사건발생의 예상비용에 대한 정보만 있으면 년간예상손실액(ALE)을 확정할수 있다. 기성위험분석은 위험분석 및 관리를 위한 강력한 수단으로 되지만 사람, 교통상태와 같은 정적이거나 속도가 매우 느린 체계나 지층현상을 분석할 때에는 그 효과가 최고에 달한다. 콤퓨터기능상실을 가져 오는 사고 같은것들은 도표화하기도 힘들거니와 예측하기는 더욱 힘들다. 그 두가지 리유는 ;

1. 콤퓨터와 관련된 최근추세의 변화가 너무 빠르므로 그 어떤 지적인 예측을 위해 리력자료를 충분히 수집한다는것은 곤난하다. 이에 대한 좋은 실례는 정전으로 인하여 체계의 가동이 중지된데서 볼수 있다. 캘리포니아의 한 관찰자는 어느 한 봉

사기관리업체가 10년내에 3시간짜리 정전상태가 1회이상 있을것으로 추측하였다. 1996년에 그 추측이 그럴듯 하였다. 그로부터 5년도 안되여 전력위기가 계속된 후 그 예상회수는 10배로 늘어 났다.

2. 콤퓨터범죄에는 호상작용하는 특성이 있다. 범죄자들은 어느 한 기업에서 보호상태가 가장 약한곳을 타격하려고 한다. 정보보안팀의 대응으로 하여 한번 공격받은 곳은 인차 보강되군 한다. 공격자들과 공격받는 사람들사이의 이러한 관계로 하여 예측시도가 상당히 탈선되는 경우가 많다.

정보위험이 기타 기업위험과 같은점들이 많지만 정보위험도 독특한것이므로 기성방법으로 분석하고 문제를 해결하는것은 상당히 어려운 문제이다.

최선을 다하여

전자상업거래활동을 보호하기 위하여 대부분 기업들은 방화벽과 인증체계와 같은 요소들에 초점을 두면서 처음부터 《피하기》전략에 매달렸다. 인터네트의 교묘한 리용에 대하여 매일 매시각 들리는 소식은 이 피하기전략이 절대적으로 필요하지만 충분한 방어로는 되지 못한다는것을 보여 주고 있다. 침입사건이나 고장발생시에는 이 피하기전략에 매달려도 별로 소용이 없다. 침입이나 가동정지를 피하기 위해 최선을 다하지만 이런 현상은 계속될것이다. 전자상업거래라는 위험률이 큰 세계에서 앞으로 살아 남으려면 이것을 알아야 할뿐아니라 그에 대처할 준비도 있어야 한다.

인터네트침입에 대한 보도는 빈번하며 때로는 충격적이여서 경영진의 관심을 끈다. 할수 없이 회사경연진과 정보보안담당회사들의 머리속에서 나온 가장 흔히 쓰는 대응책이란 현행노력을 단순히 배가하는것뿐이다. 무서움에서 출발한 이 반응은 부분적인 성과밖에 달성하지 못할것이다. 기관내에 새로운 기구를 설치하여 인터네트범죄자들보다 한수 더 뜨려는것은 불가능할뿐이다.

보안전략의 실패를 가장 잘 보여 주는 계측자료는 재정적지표이다. 어느 한 소식통에 의하면 방어프로그람 및 설비에 드는 자금은 2004년까지의 2년기간에 55%로 뛰여 올라 전국의 업체들에서 197억딸라 수준에 이를것으로 추산되고 있다. 콤퓨터보안예산이 증가하는것과 보조를 계속 유지하는것이 바로 콤퓨터범죄의 실질적인 효력이다. 콤퓨터범죄의 피해범위와 그 회수가 얼마나 극적으로 증가되였는가를 콤퓨터보안연구소(CSI)와 련방수사국(FBI)이 공동으로 작성한 최근의 년례조사보고서에서도 잘 알수 있다. 조사에 응답한 273명이 총 2억 6천 500만딸라의 손실을 보았다고 한다. 이 수자는 지난해에 보고된 1억 2천만딸라에 비해 훨씬 증가한것이다.

조사결과가 그 현상에 대한 절대적인 척도로는 될수 없지만 굉장히 증가하였다는 보안지출도 50%계선에 있으며 콤퓨터관련범죄로 입은 년간물질적손실액이 이 보안지출액보다 훨씬 더 많다는것을 생각하면 소름이 끼친다.

늘어 나는 범죄적손실의 뒤꽁무니를 따라 가는 보안에 드는 막대한 비용을 종합적으

로 보면 전자상업거래의 장래는 어둡게만 보인다. 보안상 위협에 대하여 적극적인 대책을 강구하지 않으면 보안관리의 무질서로 하여 정상이던 회사들이 몰락하게 될것이다. 해커의 공격을 당하지 않고 피할수 있는 회사들은 엄청난 보호비용에 마침내는 굴복할수도 있을것이다.

일 반 상 식

누가 소들을 놓아 주었는가

1990년대 정보보안관리를 맡은 사람들속에서는 보다 포괄적인 전략에 낯을 돌릴대신 부정적인 보안사건의 예방에만 몰두하는 경향이 나타났었다. 이런 예방을 중시하는데는 3가지의 뚜렷한 리유가 있었다.

- 사고회복보다 사고예방에 비용이 덜 든다는것이 경험으로부터 얻은 교훈이라는것이다. 《소 잃고 외양간 고친다》는 격언이 이것을 가장 뚜렷이 표현해 준다. 수복작업(이 경우는 소들이 다 뛴다음에야 소들을 다 모아 들이는것)이 미리 문에 단단히 열쇠를 잠그는것보다 훨씬 더 부담이 크다는 뜻이다.
- 비밀성의 상실은 수복할수 없으며 따라서 그에 대한 확고한 담보도 없었다는것이다. 비밀정보의 가치평가는 역설적이다. 일부종류의 기밀정보의 총체적가치는 공개되면 령으로 된다. 반대로 어떤 정보는 일정한 상태 례하면 입력하여 처리한후 출력도표(IPO)에 나오든가 아니면 합쳐지는 경우 그 가치가 굉장히 뛰여오른다. 이와 같은 극단한 경우가 있어 《몽땅 가져 가든지 아니면 다치지도 않는》심리가 작용하는 실례들이 많았다.
- 수복기능보다 《요새》기능(보호기능을 의미함)이 경영진에는 더 쉬운 구매로 되여 왔다는것이다. 정보보안관련쏘프트웨어는 언제나 잘 팔리지 않는다. 얼마 도움도 안되고 또 원래 값이 비싸다. 현실적인 방법 즉 우발적인 사건들이 어떠어떠하니 보안체계는 이것을 피하라는식의 방법으로는 그 매상고를 늘이지 못할것이다.

첫 론거가 비슷하다. 피한다는것은 결국 일이 저질러 진후에 그것을 수습하는것보다 비용이 적다. 리론상으로 볼 때 더 좋고 새로운 방어장치 및 프로그람을 갖다놓고 더 령리하고 숙련이 잘 된 일군들을 배치하여 그 프로그람들과 설비들을 감시하게 한다면 문제가 응당 생기지 말아야 한다. 그렇게 되자면 또한 보다 안전한 작업장으로 되여야 한다. 그러나 콤퓨터범죄의 폭발적인 증가가 보여 주듯이 실태는 정반대이다.

《요새》방법은 그 기대에 보답하지 못하였다. 이것은 기술이 충분치 못해서가 아니다. 문제는 감행된 위협의 성격에 있다. 한 기업의 정보자산을 보호할 책임을 진 보안팀

에 있어서 항상 골치거리로 되는것은 새로운 기묘한 공격수법이 개발되는 속도이다. 이러한 급속한 속도의 증가요인은 세계적으로 거의 무한수의 해커들이 진행하는 《자원로동》에 있다. 인터네트에 대한 공격은 게릴라전의 최종적인 《모범》이다. 공격들은 통일성이 없으며 해커대군은 무형인데다가 그 분견대들사이의 통신은 그야말로 몇초사이에 이루어 진다. 100%의 보호가 담보될 정도의 전반적이며 최신식인 방화벽이나 침입탐지체계란 없다. 방어체계가 최신의것으로 효력을 잃지 않으려면 해커들에게 기묘한 도구를 실행시키기전에 알려 달라고 요구하는수밖에 없다. 어처구니없는것으로 보이겠지만 실태가 이 정도이면 방어체계의 개발주기가 얼마나 짧은것인가를 쉽게 알수 있다. 흔히 해커들이 묘한 도구를 실행시키고 그 다음에야 그것이 탐지되고 또 그 다음에 결국 리해된후에야 그에 대한 방어체계가 겨우 만들어 지는것이다.

콤퓨터범죄자들에 대하여 보도매체들이 상당히 매혹을 느끼지만 사실상 실지 관심을 돌려야 할것은 그 범죄사건이 일어 난후의 《영웅전》이다. 대용량전자상업거래싸이트가 공격받을 때 구경군들(특히 피해입을 주주들)은 그 《영웅적》업적의 세부에 대해서보다 그 싸이트가 얼마나 오래 걸려야 복구되며 다른 장애가 또 있겠는가 하는데 더 관심을 돌린다. 우스운 일이지만 이렇게 사회적호기심이 커도 사건대응 및 수복용자금은 보안예산과 전자상업거래예산에서 력사적으로 제대로 받아 본적이 없다.

정보보호전략을 재검토하여 현 위기상태에 부합되게 할 때는 지금이다. 인터네트상에서 기업을 운영하는 기관들은 수시로 정보보호전달을 수정하여 범죄자들의 악성적인 공격과 자연재해 기타 사고들로부터 수습대책을 세울 가능성들을 항상 고려해야 한다. 수복작업을 위한 적절한 준비를 한다는것은 비용이 많이 들지만 기업에 절실한(시간적으로 절실한) 인터네트봉사형태들을 위해서는 절대적으로 필요한 사업이다.

표 23－1에서는 정보보안방어체계의 간단한 계층 3을 제시하고 있다. 방어체계에서 가장 중요한(또한 투자를 요하는)것들은 아래의 3가지인데 여기서 마지막 항목인 회피가 가장 큰 부분이다. 전자상업거래활동을 잘 보호하자면 기관들의 수복문제를 포함시키고 담보와 탐지를 보강할 필요가 있다.

표 23－1　　　　　정보보호모형

준 위	실　례
수복	사건대응, 재해수복
탐지	침입탐지
담보	취약성분석, 기록부검열
회피	방화벽, 공개열쇠기반(PKI)방책, 표준제도

또 다른 난문제인 기업지속관리

기업지속관리(BCM: Business Continuity Management)는 정보보안의 작은 부류로서 수복을 위험관리의 일차적인 방법으로 해결하는 분야이다. 정보보안의 다른 분야들이 지금까지 예방에 주력하여 왔다면 BCM은 거의 일방적인 방법으로 수복에 초점을 두어 왔다. 보안이 사건후의 전략에 자기의 초점을 넓혀 나가야 한다면 영업지속은 자기의 초점을 넓혀 사건후전략까지 다 포괄할 필요가 있다. 전자상업거래시대에 BCM은 회피전략을 고안하여 기업을 효과적으로 보호할 필요가 있다. 그 리유는 시간이다.

인터네트기업의 사용상요구를 검토해보면 놀라운 사실을 알게 된다. 즉 운영정지로 인한 만회할수 없는 손해를 봄이 없이는 수복시간이 모자란다는것이다. BCM이 지금까지 수복전략에 의거하여 체계리용성유지를 해온것만큼 전자상업거래에 대한 요구로 하여 불피코 수복이 불가능한 선택이 아니겠는가 하는 생각이 든다. 그 리유는 최고허용정지시간(MTD: Maximum Tolerable Downtime)이라는 기초변수가 명백히 밝혀 준다.

MTD는 기업이 받은 재정적, 운영적 및 명예적인 손실을 수복하기 위하여 체계를 얼마만한 시간동안 정지시켜야 하는가를 재는 척도이다.

전자상업거래는 이 MTD를 단축하여 일부 경우에는 령으로 만들었다. 몇해전에 어느 도매상점체계에 재해가 나서 수복날자가 며칠 걸릴번한 일이 있었다. 매일 24시간 매주 7일간의 중단 없는 전 세계적봉사의 도입으로 하여 재해를 복구할 때 가동중지시간은 단 몇분밖에 허용되지 않는다. 이 경우에는 어쩔수 없이 유일한 수복방도인 회피전략에 들어 가는수밖에 없다.

표 23－1에 제시한 정보보호모형을 다시 참조해보면 BCM이 보다 필요로 하는것은 계층구조의 마지막 아래부분의 회피분야에 있는 해결대책이다. 이 부분의 해결책들을 언급하는것은 이 장의 분야가 아니지만 리용성제고의 실례에는 예비체계, 체계이중화, 고장퇴치, 지리적으로 떨어 진 곳들에 자료를 복사해 두는 사업 등이 포함된다고 말할수 있다. 중시하는 점이 달라 졌다고 하는 또 하나의 실례는 기업지속이 최근에 담보와 탐지에 더 큰 투자를 요구하고 있다는것이다. 2002년에 해커공격이 물리적인 공격으로 되는것과 관련하여 회사들의 Web참가률이 떨어 질것으로 예견된다. 기업지속팀들은 한때 말단사용자나 문의봉사소에서 오는 전화를 받고야 체계고장을 알군 하였다. 그러나 오늘 정교한 감시수법과 탐지수법이 있음으로 하여 각 기관들에서는 공격에 신속히 대응하여 지속적인 손실을 미리막을수 있게 되였다.

기업지속팀구성도 역시 이러한 새로운 현실이 반영되게끔 변화시켜야 할 필요가 있을것이다. 10년전에는 영업지속전략이 대체로 주제를 다루는 전문가들이나 전문적인 기업지속계획작성자들의 전공분야에 지나지 않았다. 2000년 2월에 있은 분산형봉사거부공격으로 하여 방화벽전문가, 경로기조종자, 사건관리전문가들로 무어 진 특별팀들이 우후죽순처럼 생겨 났다. 이 팀들은 기업지속성에서 문제로 되는것은 무엇인가에 대하여 의견을 모았는데 그것은 체계리용성의 상실이였다.

기업의 방어체계를 재정비하여

1990년대 중엽까지만 돌이켜 보아도 정보위험관리에서 큰 문제가 없어 상당한 진보가 이룩되고 있었던것으로 생각된다. 기업들의 보안에 대한 위협은 앞으로 분명히 있을것이라는것을 예상하였으나 당시에는 기술적발전이 이것을 꼭 제약할것으로 모두 믿었다. 그런데 유선분야에서 비안전성이 있어 정보보호를 엄격히 통제해야 되겠다는 귀에 거슬리는 소리로 하여 우리는 현실에 눈을 크게 뜨게 되였다. 파도처럼 계속 밀려 드는 악착한 공격과 그칠새 없는 영업중지를 보면 아마 오랜 기간이 지나야 다시 안심할수 있겠다는 생각을 하게 된다. 그러나 용기를 잃지 말아야 한다. 모두가 경각성을 높인데다가 현 위험상태를 엄밀히 분석해 보면 우리는 앞으로 힘 있게 전진할수 있다고 보아 진다. 그러나 명백한것은 지난 몇해동안 리용하여 기반이 든든하지 못한 꼭 같은 전략을 계속 추구한다면 그 어느 기관이든지 자기들의 기업환경에 대한 보호를 어느때 가도 갱신하지 못한다는것이다. 전자상업거래시대에 우뚝 솟아 오르려면 진지들을 검토하며 낡은 전략들을 버려야 할것이다.

기업의 방어체계에 대한 재정비에서 중요한것은 재설치가 아니라 재고려라는 사실이 우리로 하여금 큰 고무를 받게 한다.

필요한 대부분의 기술들은 이미 기업들이 가지고 있거나 쉽게 구입할수 있다. 기관들의 방어전략의 검토를 건의하는데서 4가지 주요분야에 대한 분석이 필수적이다. 아래에 그 4가지를 제시하였다.

보안구조

기관의 보안구조를 정확히 구축하려면 기관의 기본업무기능들에 대한 전면적인 리해가 필요하다. 이에 대하여 리해를 하려면 기관내의 업무일군들과 담화를 하는것이 가장 좋다. 업무기능들을 료해한 다음 그 기본기능들을 정보기술봉사형태들과 련결시킨다. 이것들은 또 외부의 공격, 간첩행위, 체계가동정지로부터 보호해야 한다.

정보보안봉사와 정보보안체계에 대한 보호는 보안실천과 보안대책을 실행하여야만 달성된다. 그러므로 보안구조의 연구결과는 정보보안그룹의 활동을 회사의 기본업무와 련결시켜 보아야 한다.

보안구조의 연구결과들은 인터네트에 최근에 뛰여 든 기업들에 있어서 절실한 계몽사업이다. 기업들은 보안공정들과 장치들을 가지고 있어 2차적인 중요성을 띠는 분야들은 보호하고 있지만 새로운 분야 즉 기업에 사활적인 분야들은 보호 없이 그 운영이 진행되고 있다. 효과적인 보안구조모형을 작성하면 보호가 가장 필요한 그 분야들에 충분한 자원을 집중할수 있게 된다.

보안구조연구의 결과가 가지는 또 하나의 보충적인 우점은 그의 교량적기능에 있다. 보안구조는 정보보안과 그가 보호하는 영업기능들사이의 관계를 세밀히 추적분석하여 정보보안이 기업에 얼마나 큰 가치를 가지는가를 제시해 준다. 그로부터 오는 새로운 가치있는 안목으로 하여 예산작성에서 명확한 요구를 제기할수 있을것이다.

기업영향분석

기업영향분석(BIA: Business Impact Analysis)은 지금까지 몇해동안 기업지속계획작성에서 하나의 핵심분야로 리용되여 왔다. BIA는 그 어떤 체계의 단위시간동안 가동정지의 비용을 추산한다. 이 비용을 추산해 내면(례하면 하루 10만딸라) 체계보호와 관련한 과학적인 결심이 마련된다. 이 정보는 이렇게 쓰이는 외에도 있을수 있는 가동정지비용에 대하여 회사측에서 보호대책용지출에 인차 응해 나서도록 하는 결심채택보조수단으로도 쓰인다.

극히 최근까지만도 BIA는 기업지속계획작성자들에게만 쓰이는 하나의 도구였다. 전자상업거래리용에 대한 악질적인 공격들이 점차 손해를 많이 주는 형태의 콤퓨터범죄로 됨에 따라 BIA는 점점 더 광범위한 관심을 모으고 있다.

전자상업거래체계에서 기업영향분석을 하는것과 관련하여서는 두가지 문제점들이 강조되여야 한다.

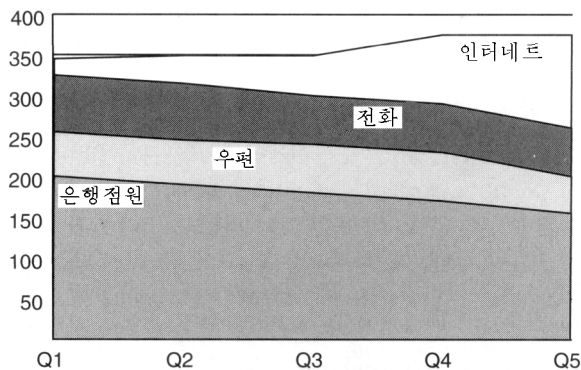
첫째로, MTD가 령으로 접근하게 되면 기업영향의 잠재성은 절대와 무한으로 되여 점근선과 매우 류사하게 될것이다. 여기서 그 체계의 실지작용에 대한 리해를 정립할수 있다. 인터네트에 련결된 너무나도 많은 체계들이 증권거래 같은 실시간활동을 주관하고 있으므로 그 어떤 체계의 가동정지의 영향은 즉시에 파국적인 후과를 빚어 낼수 있다. 이전에 보다 완화된 수복조건을 제공하던 호스트체계인 백오피스(back–office)에서도 사정은 마찬가지이다. 실시간인터네트영업모형으로 이행한것과 관련하여 매주 7일간 매일 24시간요구사항은 낡은것으로 될지도 모른다. 그로 하여 난관이 제기되면 그 기업이 일정한 가동환경상에서만 영업을 할수 있게 하는 능력과 관련한 결정들이 생겨 날수도 있을것이다.

한 은행의 총 거래대역이 분기당으로 100만딸라단위로 표기됨. 4개형태의 거래를 합하여 총액을 산출함. 소득흐름이 원천마다 다르므로 매 분야에서 고장난 체계가 은행에 주는 물질적영향은 그 변화에 비례하여 증가 또는 감소되여야 한다. 그러므로 BIA에서 쓰는 수자들은 변화를 고려하여 가져다 써야 한다.

그림 23－1. 시기별 은행업무봉사

둘째로, BIA가 여러개의 소득흐름을 잠재적손실리윤의 원천으로 사용하기때문에 영업이 인터네트로 이행함에 따라 자주 갱신해 줄 필요가 있다. 즉 실례로 전화쎈터를 인터네트를 리용한것으로 바꾸려는 회사는 중요성이 적어지는 전화쎈터에 미치는 영향을 고려해 보아야 한다는것이다. 이렇게 하려면 BIA를 항상 시간갱신하든가 아니면 예상곡선을 리용하여 미래의 수치들을 외삽해야 한다. 직결봉사로 넘어가는 한 은행의 실례가 그림 23－1에 주어 져 있다.

BIA결과값들을 보면 예상되는 위험이 구체적인 도달점 즉 얼마만한 자금지출을 요구하겠는가 하는것이 도출된다. 보안구조검토에서와 마찬가지로 로출된 정보는 하나의 매우 강력한 도구가 있다는것을 우리에게 암시해 준다. 자원을 확보하여 기업관리에 절실한 체계나 공정을 보호하는것은 가동정지비용이 계산되여 경영진에 제출되게 될 때만이 훨씬 쉬워 질것이다.

위험분석

위험분석에서는 개별적인 위험요소들을 일정한 체계나 공정으로 갈라서 등급을 매겨놓는다. 지난 시기에 정량적인 위험분석은 시간이 매우 많이 들고 정확성도 상당히 부족하였다. 전자상업거래분야에서는 위험분석이 신속하게 결정되여야 효과가 있다. 시장실현목적과 생산이 신속히 변화되여 리윤성을 최대로 높여야 하는 산업분야에서는 위험분석이 위험상태를 피하는데서 관건적역할을 한다. 솔직한 관찰과 가공하지 않은 제안들을 내놓음으로써만 위협을 피하고 대처하기 위한 전략을 세울수 있게 된다.

촉진적위험분석이라는 방법(콤퓨터보안연구소에서 개발한)을 쓰면 불필요한 세부에 빠져 드는 경향을 피하고 위험을 직선적으로 빨리 확정해 낼수 있다. 이 방법을 사용할 때 촉진자는 대체로 6~12명으로 구성된 작은 그룹을 지도하여 해당 체계에 대한 위험들에 대하여 성원들의 인상을 불러 일으키는 식으로 여러가지 질문들을 제기하여 대답을 받는다. 리상적으로는 그룹이 서로 다른 부류의 사람들로 구성되여 그 체계에 대한 독특한 자기식의 견해를 가지면 더욱 좋다. 매 사람들이 진행하는 평가가 실시간적으로 동등검토로 되는것으로 하여 이 과정은 집단인터뷰와 자못 류사하다. 여기서 나온 결론은 체계의 주요위험요소들과 그 요소들을 약화시키기 위한 여러가지 통제대책안 등으로 종합되게 된다.

하나의 과정으로 볼 때 이 촉진적위험분석은 상당히 가벼운 공정으로서 해당 그룹에 지나친 부담을 주지 않으면서도 필요할 때마다 자주 반복할수도 있다. 정보보안관리를 잘하는것은 기업의 정보에 주는 위험요소들을 현실적으로 그때그때 분석하는데 달려 있다. 또한 정보보안팀의 사명이 고객의 기대에 어긋나지 않도록 담보하는 하나의 주요한 방도로도 될것이다.

사건대응

20년전에는 사건대응이 순수 재해복구와 기업(물리적)의 보안분야에서만 언급되였다. 큰 체계사고였을 때에는 복구팀이 구체적인 공식계획을 작성하여 정보자산을 복구하였다.

사고의 리유가 의심되면 수사관을 채용하여 그것을 수사하군 하였다.

의뢰기 및 봉사기망과 개인용콤퓨터망들이 출현하여 무수한 취약점들이 산생됨으로써 내부망과 호스트를 보호하기 위한 예방적인 대책들을 취하지 않으면 안되였다. 정보보안공장들이 새 기술의 물결을 타고 앞으로 질주하게 되였으므로 회피는 여전히 좋은 전략으로 되였다. 그러나 비상복구가 새로운 현실로 자기 모습을 드러내였다. 사실 대부분의 기관들은 오늘날 끔찍이도 소란을 피우며 사고복구를 하고 있는것이다.

오늘 대부분의 공장들에서는 사건대응이 정보보안에서 가장 약한 고리로 된다. 사건복구는 기관의 정보체계에서의 무계획적인 부정적사건을 탐지하고 대응하는 능력이다.

대부분의 회사들은 회피에 대한 믿음이 확고하지 못한것으로 하여 사건대응준비가 비참할 정도로 미약하다. 믿음직한 망의 주위에 난공불락의 성벽을 쌓는 현상이 지난 10년간 너무나도 만연되여 사람들은 콤퓨터범죄를 발견하고 그 후과를 회복하는데 비용을 쏟는것이 경솔한 자금랑비라고 생각하게 되였다. 이것은 《타이태니크》호의 려객들 절반에게만 구명정을 보내는것과 같은 천진성과 기술적신뢰가 결합된 심리에 기인된다.

대부분의 회사들에서 사건대응능력이 놀라울 정도로 없는 현상은 콤퓨터범죄의 한부분인 내부범죄를 놓고 볼 때 더욱 뚜렷해 진다. 콤퓨터보안연구소와 련방수사국이 공동으로 진행한 콤퓨터범죄조사보고서는 지난 몇해동안 콤퓨터범죄가 얼마 변하지 않았다는 것을 놀랍게 보여 주고 있다. 보고서를 보면 거기에서 밝혀 진 사건의 약 70%가 회사내부사람들이 감행한것이라는것을 알수 있다. 그 수자들이 과장되였다 할지라도 탐지 및 대응능력은 상당히 제고할 필요가 있다. 이 경우들에 범죄자들은 방화벽의 《안온한》쪽에서 발견되였다.

이러한 위험들이 억제되지 못한것은 최근에 인터네트보안에 드는 비용이 상당히 증가된데 있으며 이 위험들을 제거하자면 탐지하고 대응할수 있는 전문기술문제가 해결되여야 한다.

사건대응은 정보보안이라는 격납고에 핵심적인 요소를 하나 제공하게 되는바 이것이 바로 한 그룹을 무어 복잡한 정황을 분석하고 대응대책을 강구케 하는 조직적능력이다. 운영을 잘하면 사건대응계획으로 하여 기관전체가 재해에서 구원될수도 있다. 그러한 팀은 각이한 분야의 전문가들 즉 법전문가, 망전문가, 보안전문가, 선전분야의 전문가들을 망라하면 더 좋을것이다. 그리고 기관에서 그 팀에 정기적으로 훈련을 줄 필요도 있다.

결 론

정보보안제품들과 봉사에 대한 요구가 끝없이 높아 지고 있지만 콤퓨터범죄로 인한 총 손실액은 보안지출을 릉가하고 있는것으로 보인다. 이것은 보안전략을 철저히 재검토할것을 촉구하고 있다. 그런데 회사들의 정보보안관리자들은 보안용지출을 더 높여 더 강한 울타리를 구축하려고 헛되이 시도하는것으로 생각된다. 최근년간의 경험으로 보아 이 계획에 대하여 지나치게 락관적인 태도를 취할 필요는 거의 없다고 본다.

인터네트는 거의 모든 산업에서 거래업무공정들을 실시간적으로 주관해 나간다. 지금까지 회사의 기술적 및 재정적내역이 생각지 않게 공개되여 버리는 현실은 21세기 정보일군이라면 누구나 매일 체험하는 일로 되고 있다. 정보위험관리는 한때 몇명 안되는 결심채택자들과 보안기술자들로도 가능한것으로 알려 졌다. 이런 시대는 이미 지나갔다. 위험과 급변으로 가늠할수 없는 오늘의 환경에서 위험관리를 해나가려면 명철한 사고와 넓은 경험적토대가 필요하다. 이것은 정보보호를 위해서는 특별한 대책들을 강구할뿐아니라 이런 대책이 실패할 경우에도 대처할수 있게 준비를 할것을 요구한다. 또한 기업내의 많은 부서들이 참가하는것도 적극 장려해야 한다.

영향력 있는 지위에 있는 사람들은 보다 포괄적인 방어체계구축을 힘 있게 내밀어 주어야 할 책임을 지니고 있다. 인터네트시대에 성공의 열쇠는 다름아닌 부정적사고를 피하여 그런 사고를 회복할수 있는 준비가 된 강력한 보안기초시설구축에 달려 있다. 20세기에 위험관리는 사건후대책(탐지와 수복)뿐아니라 사건전대책(회피와 담보)에도 관심을 잘 돌릴것을 요구한다. 과업은 아름차나 이미 잘 리해하고 있으면서도 잘 리용하지 못하였던 기술을 어떻게 적용하는가 하는데 바로 성과가 달려 있다.

참 고 문 헌

1. Prince, Frank, Howe, Carl D., Buss, Christian, and Smith, Stephanie, Sizing the Security Market, *The Forrester Report,* October 2000.
2. Computer Security Institute, *Issues and Trends: 2000 CSI/FBI Computer Crime and Security Survey,* Computer Security Institute, 2000.

제２４장. 기업내 정보보안

류언 이. 샤프

기업에 있어서 정보의 가치는 아무리 과장하여도 무리가 아니다. 특히 오늘의 지식화된 경제에서 더욱 그렇다. 정보는 많은 기관들에 있어서 가장 귀중한 유일한 재산이라고도 할수 있다.

기업의 자료자산들은 지리적견지에서 보나 경영진의 견지에서 보나 이전에 비하여 상당히 분산되여 있다. 또한 기업의 자료를 보려는 내부사용자들의 수가 늘어 났으며 전통적으로 공고하던 정보기술의 령역이 보다 쉽게 접근되는 경향도 적지 않다.

정보관리의 하나의 목적은 말단사용자 즉 고객들에게 가치가 높은 정보봉사를 제때에 하는것이다. 정보는 그 시간적리용성에서 그리고 안전한 리용성에 비례하여 가치를 가진다.

어지럼증이 날 지경으로 이러저러한 제품들과 기술들이 쓸어 나와 정보보안을 각이한 형태로 각이한 복잡한 환경에서 보장하여 준다고 하는 조건에서 최선의 해결책은 종합적인 보안틀거리를 작성하는것이다. 이 틀거리는 기업전반의 요구에 맞게 보안을 효률적으로 반영할것이다.

이 장에서 언급될 문제점들은 다음과 같다.

- 보안의 필요성
- 보안실행의 요구조건
- 최량적보안틀거리의 특징
- 보안요구조건을 만족시키기 위한 주요기술적대안
- 기술과 요구조건을 일치시키는 효과적인 보안틀거리의 구축

보안의 필요성 : 회사자료들을 분석해 보며

세계의 수많은 지역들에서 해커들의 지하망들은 인터네트상에서 전송되는 자료들을 가로채거나 수정할수 있는 매우 정교한 도구들을 개발하여 뻐젓이 공유하여 왔다. 이러한 도구들을 써서 회사사무실건물이라는 상대적으로 안전한 성벽안에서도 자료를 엿듣고 가로채는 현상이 나타났다.

엿보기(sniffing), 가로채기(hijacking), 위조하기(spoofing)에 쓰이는 도구들은 인터네트상에서 공개적으로 구입할수 있다. 원래 정보의 자유로운 교환을 위하여 공개된 수단으로 창설된 이 인터네트는 세계적으로 흐르는 자료들의 흐름에 많은 사람들이 접근할수 있는 기회를 주고 있다. 실례로 한 사람이 먼 곳에 있는 자기 친구에게 보내는 전자우편 하나가 자기 목적지까지 도착하려면 수많은 중간《마디》들을 《건너뛰기》하여야 한다. 가는 도중 어느 지점에서나 그 전자우편의 내용이 보여 질수 있는데 특히 경쟁자, 대리

인도 볼수 있으며 협잡을 목적으로 하는자도 그것에 접근할수 있게 된다.

지난 몇해동안 해커들의 인터네트상에서의 공격위험은 사회에 널리 알려 지게 되였으며 그중 몇가지 주요해킹사건으로 하여 기업과 정부의 사업과 운영이 중단되기도 하였다. 사실 초기의 조사결과를 보면 모든 침입사건들중의 50%이상이 기관내부에서 일어날것이라고는 하지만 해킹사건에 대한 최근 분석에 따르면 이러한 경향이 방향이 바뀌고 있는것으로 보인다. 이 연구자료들은 다수의 공격이 기관밖에서 오는것으로 평가하고 있다. 이러한 공격이 진행되여도 모르거나 보고되지 않는것이 너무 례상사로 되여 통계학적수치들이 그 위협의 심각성을 과소평가하고 있는지도 모른다.

콤퓨터보안연구소가 진행한 광범한 부분의 2,213개의 Web싸이트들에 대한 최근의 한 분석결과에 의하면 일부 상용싸이트들중 28%가 공격에 《상당히 취약한》것으로, 30%가 일정하게 취약한것으로, 오직 42%만이 안전한것으로 밝혀 졌다. 조사한 싸이트들을 6개의 부류로 즉 은행, 신용조합, 미련방싸이트, 신문, 성인싸이트, 기타로 분류하였다.

다른 하나의 최근 연구에 의하면 1997년부터 1999년까지기간에 자료나 망관계파괴사건이 매해 35%이상으로 증가된것으로 회사들은 보고하고 있다. 이 연구에서 또한 기관들이 보고한데 의하면 매해 25%의 금융사기행위가 직결상에서 감행되였다고 한다. 내부사람들이 망접근을 오용한 건수는 25%이상으로 증가하여 800만딸라의 손실을 가져 왔다고 한다.

이 연구자료들은 인터네트와 내부망으로 흐르는 회사자료의 비법적인 접근과 사용을 통한 금융사기사건으로 하여 회사들이 받는 위협이 얼마나 심각한가를 보여 주고 있으며 안전한 망환경을 보장하여야 할 필요성을 강조하고 있다.

정보보안요구사항

보안이 정보를 다루는 여러 준위에서 지켜야 할 사항이지만 많은 경우 보안실천에서는 모든 준위를 고려하지 않고 다만 특정한 문제해결에만 초점을 두고 있다. 실례로 많은 기관들에서는 인증(사용자가 본인이 맞다는 확인)과 같은 문제들의 해결이나 고객자료기지와 같은 구체적인 자원보호에만 신경을 써왔다. 이 해결방안들은 종합적으로는 사업에 상당히 좋은 도움을 주는 경우도 있다.

그러나 이 방안들은 분산분리된 부속품처럼 완전무결성이 부족할뿐아니라 사용자와 관리대면부가 서로 다른것으로 하여 사용과 유지에서 비용이 많이 들수 있는것이다.

그렇다면 정보관리자는 어떻게 해야 사용자들을 혼란시키지 않고 현재봉사를 지연시키지도 않고 또 현재예산을 깨지 않으면서도 기업정보자산의 손실을 가져 올수 있는 가능성들을 줄일수 있겠는가, 대답은 간단하다. 즉 기업의 종합적인 정보보안틀거리를 구축해야 한다는것이다. 즉 현존정보기술환경과 미끈하게 결합되는 종합적인 보안기초시설을 구축하고 가장 필요한 부분부터 그것을 점진적으로 실행해 나가야 한다는것이다.

보안틀거리의 일부 구체적인 사항들을 이 장에서 설명하려고 한다. 이 장에서는 먼저 효과적인 보안틀거리의 일부 요구사항들을 검토하고 이 요구사항을 만족시키기 위한 일부 기법들을 종합적으로 보려고 한다.

기초적인 보안기능

정확한 보안틀거리를 위한 다섯가지 기초기능들은 다음과 같다.

1. **인증** 사용자들의 신원을 믿음직하게 밝혀 보증하는것
2. **접근조종** 합법적인 사용자들만 해당자원에 접근할수 있게 하는것
3. **사적비밀보장** 합법적인 대상들사이의 통신과 체계내의 자료에 대한 비밀성을 담보하는것
4. **자료의 무결성보장** 통신내용, 파일, 프로그람을 제멋대로 수정조작하지 않도록 하는것
5. **부인방지기능** 해당 사용자가 해당 통보문을 보냈다는 부인할수 없는 증거를 제공하며 수신자가 다른 통보문을 받았다는것을 방지하는것

비루스방지와 같은 기능들은 따로 제기할 기능은 못되는것으로 본다. 그것은 이 기능이 무결성, 접근조종, 인증기능들과 대체로 결부되는것이기때문이다.

인증

전자통신을 하는 하나의 대방이나 여러 대방들의 신원을 확인하는 과정인 인증은 대방으로 하여금 신원에 대한 증거를 제시하게 한다. 즉 그들의 머리속에 있는것, 몸에 지니고 있는것 혹은 그들의 신체적특성들이 그 증거로 된다. 개인들이 육체적으로 현지에 있어 신원을 제시할수 있는 경우에는 이 특성들은 사람의 육체적특징들인 생체계측지표의 형태로 제시될수 있다. 실례로 지문, 음성기록이나 망막스캔을 들수 있다. 여기서 처음의 두가지가 가장 많이 쓰이고 있는데 그것은 상대적으로 실행하기가 쉽기때문이다.

그 어떤 생체계측형태의 신원자료를 처리할수 없는 통신환경에서는 가장 쉬운 방법이 간단한 통과암호를 쓰는것이다. 인증을 위하여 여기서는 사용자에게 알려 진 통과암호를 제시할것을 요구한다. 통과암호에 대한 인증이 잘 되려면 안전한 통로를 리용하여 망으로 암호화된 통과암호를 전송하여야 하며 그렇지 않으면 전자도청수단에 의해 통과암호가 롱락당할수도 있다.

통과암호자체는 그리 안전하지 못하다. 대체로 짧고 기억하거나 옆에서 보기 쉽다. 일정한 형태의 수자식상업형태에서는 지금까지 가장 약한 고리가 바로 통과암호였다. 또한 각이한 체계에 수많은 통과암호를 쓸것을 요구하므로 사용자들이 모든 접근요구사항에 하나의 통과암호를 쓰는 경향이 지배적이였다. 사용자들은 거의 모두 자기의 통과암호를 써놓은 목록에서 하나를 선택하여 쓰든가 아니면 모든 통과암호를 다 종이쪽지에 써서 콤퓨터옆에 놓고 쓰기가 일쑤이다. 이 두 경우가 매우 위험한 경우로서 다른 사람이 모든 체계들을 단번에 다 녹여 낼수 있는 가능성이 매우 높다.

효률성이 높은 인증방식은 통과암호(본인이 알고 있는것)와 늑은 스마트카드식통표(본인이 지참하고 있는것)를 결합시키는것이다. 그 대표적실례가 바로 ATM(자동현금출납

기)카드이다. ATM카드는 본인이 직접 가지고 다니는것이며 PIN(개인식별번호)은 본인이 머리속에 가지고 있는것이다. 결합을 잘하면 하나 쓰는것보다 보호가 더 잘 될수 있게 된다(두 요소인증).

인증의 중요한 측면의 하나는 인증이 단일방향적인것(보내는 사람이 봉사기에 인증을 하는것)인가 아니면 쌍방향적인것(사용자와 봉사기가 서로 인증하는것)인가 하는 문제이다. 실례로 한 은행지점에 있는 ATM을 사용할 때 그것이 합법적인 ATM이라고 가정한다. 그러나 주차장에 홀로 서 있는 ATM을 사용할 때 그것에 대해서도 꼭같은 믿음이 가겠는가가 문제이다. 도적들이 극히 신뢰성이 가게 만든 가짜 ATM을 주차장들에 건설하였다는 문건화된 사건기록도 있다. 현금은 물론이고 ATM카드와 PIN을 순진한 사용자들에게서 수십개나 가로채간것이다. 이러한 사기행위들이 믿건대 드물다고는 하지만 이것을 보면 쌍방향적인 인증의 필요성을 절감하게 된다.

전자적인 환경에서 공개열쇠암호화체계(흔히 공개열쇠기반 즉 PKI라고 함)에 수자식인증서들을 결합하면 호상인증을 위한 명백하고도 안전한 방도를 가질수 있다.

공개열쇠와 비밀열쇠체계들과 수자식인증서의 효력은 비밀열쇠를 어떻게 비밀에 붙이는가 하는데 있다.

만일 어떤 사람의 비밀열쇠가 도난 당하든가 비법적인자가 접근했든가 하면 그 사람으로부터 오는 통신과 그 사람에게 가는 통신은 다 손상된것으로 간주하여야 한다. 기관들에서 비밀열쇠를 개인용콤퓨터에 기억시켜 두는것은 하나의 심각한 보안위험으로 된다. 비밀열쇠가 개별적사람의 콤퓨터에 있으므로 사용자는 그 콤퓨터상에서 인증을 받아 보안을 담보해야 하는것이다. 가장 강력한 보안체계에서는 이 정보를 스마트카드에 보관하고 PIN을 써야만 접근권을 허용할것이다.

접근조종

접근조종(즉 허가 혹은 인가)은 단어그대로 사용자가 보안방책관리자의 결심에 따르는 해당자원(체계, 목록, 자료기지, 지어 기록부들)에 대한 접근권을 가지게 하는것을 말한다. 접근조종에 널리 쓰인 기술에는 접근조종목록(ACL), 단일계약제품방화벽을 리용한 믿음직한 운영체계들도 있다. 단일개시신호제품들은 사용자로 하여금 해당 환경에 대한 인증을 대화당 꼭 한번만 받게 한다. 그리하여 사용자는 그 대화기간 보충적인 인증을 받을 필요없이 해당 자원중에서 어느것이나 접근할수 있는 권한이 부여 받는다.

사적비밀

사적비밀은 어느 보안환경에서나 초석이다. 사적비밀에 대한 정의가 사용자와 소유자간에 상당한 차이를 보여 주기도 하지만 사적비밀문제는 자료가 금융적, 연구적가치나 인사문제와 관련한것일 때에는 더욱 중요하다. 회사의 내부망에서도 사적비밀문제가 중요하다. 그러나 개인 및 회사자료에 대한 일정한 접근권을 주면서도 동시에 개인들과 회사의 리익이 보호되여야 하므로 엑스트라네트에서는 자료취급과 관련하여 가장 큰 애로를 느낀다.

디스크에 보관하였건 망에서 교환되건 관계 없이 정보는 그 비밀성에 따라 불법사용자들이 해독하지 못하도록 암호화되여야 한다. 물리적으로 고립시키는 방법으로 사적비밀성을 보장할수는 있다. 그러나 오늘의 콤퓨터사용환경에서 이것은 누구에게나 다 비효률적인것이다. 리상적인 해결책은 중앙집권화가 아닌 분권적인 암호학적환경을 시행하여 매 사용자에 암호화된 정보들을 가지고 교환할수 있게 해야 한다.

전자적인 자료에 대한 신뢰사항은 전체적으로 암호화하는 토대에 의거한다. 대칭적 및 비대칭적암호화 등 많은 암호화체계들이 있다. 그러나 비대칭적암호과정은 대개 심각한 약점을 하나 가지고 있다. 즉 그것은 대칭적공정에 비하여 계산학적으로 매우 비용이 많이 든다는것이다.

이 문제를 최소화하기 위해 빠른 대칭적코드화체계가 속도가 느린 비대칭적체계와 결합되고 있으며 공개열쇠와 비밀열쇠를 결합적으로 사용하여 통신자료를 해신하고 복호화하게 된다. 안전한 환경에서 매 사용자는 공개열쇠와 비밀열쇠와 함께 사용자이름을 할당받게 된다. 공개열쇠는 사용자이름과 함께 리해관계를 가지는 모든 대상들에 공개되게 되지만 비밀열쇠는 그 소유자만 알고 있다.

정보의 무결성을 보호하는 다른 절차에서는 수자식서명을 생성하고 확인하고 비대칭코드화와 검사합알고리듬과 결합하여 이 모든것들을 효률적으로 쉽게 실행하게 된다.

그러면 해당 대상은 자료요소들에 수자식서명을 결합하는 방법으로 열쇠소유자를 인증하게 된다. 그러나 이렇게 되면 그 대상이 그 열쇠에 대응된다는것만 확인하게 된다. 이름으로 그 대상을 인증하려면 그 이름과 공개열쇠가 서로 일치한다는것을 담보할수 있는 방도가 있어야 한다. 이 문제를 개인증명서와 비교할수 있다. 즉 대상과 증명서사진사이의 일치만 보고 그 대상의 이름이 증명서에 있는 이름과 같다고 단정할수 없는것과 같다.

증명서에서와 같은 원리로부터 출발하여 전자형식의 증명서를 생각해 볼수 있다. 서로 대응되는 《신분증》은 《공개열쇠＋이름짝》을 보증하는 증명서라고 할수 있다. 또한 이름과 열쇠의 한조를 안전한 통로로 대방들에게 보내고 쓰기방지로 보존할수도 있다. 가입자나 구독자가 얼마 안되는 경우에는 모든 통신대방의 이름과 공개열쇠를 전자문서관리체계에 표로 보관할수 있다. 《중간다리》공격을 피하기 위해서는 이름과 공개열쇠가 실지 한사람의것이라는것을 담보하는것이 필요하다. 실지 이것은 이름과 열쇠쌍이 반드시 안전한 통로로 분배되고 체계에 쓰기방지되여 보관되여야 한다는것을 의미힌다.

자료의 무결성

무결성은 자료가 헝클어 지거나 파괴되거나 비법적으로 변경되지 않게 보호하는것을 말한다. 또한 설정값들도 변경되거나 조작되지 말아야 하며 각종 봉사들, 응용프로그람들, 망들의 완전무결성도 보호되여야 한다. 정보의 무결성을 보존하는것은 사활적인 문제이다. 정보가 두 대방사이에 교환될 때 그 대방들은 이 정보가 조작되지 않은것이라는 실례를 필요로 한다. 검사합정보와 개념상으로 류사하게 모든 암호화체계들은 무결성담보를 위한 효과적인 방도를 제시해 준다.

부인방지

이 요구사항은 법적론리로서의 중요성을 띤다. 내적으로나 외적으로나 점점 더 많은 기업들이 전자적운영으로 넘어 가고 있음으로 하여 전자업무거래에서 송신자에 대한 일정한 형태의 법적증거와 송신이 끝났을 때 받은 수신문에 대한 법적증거를 가지고 있게 하는것이 필요하다. 이 요구사항은 신원확인과 접근조종이라는 항목과 꼭같이 필요한 항목이다.

정보기술요구사항

보안의 기초구조가 잘되자면 우에서 이야기한 기능들이 발현되여야 하는 동시에 다음과 같은 요구사항들도 만족시켜야 한다.

- 기업전반에 걸쳐 변화되는 보안강화요구사항들
- 정보기술기반시설에 이미 구축된 보안갑문과 방화벽과 같은 점보안제품들과의 결합
- 모든 정보기술부서들에 있는 이질적인 가동환경, 응용프로그람, 망, 망설비와 도구들
- 사용자와 체계관리자들의 리용성과 능력에 대한 요구사항들
- 부서간, 지역간 및 기업간 거래
- 사용자의 사용상편리의 요구사항들
- 정보기술기관들의 통제하에서의 신축성 있고 효과성 있는 시행
- 기업전반에 걸치는 단계별시행과 배치

최상의 보안은 사용자집단에 투명하다. 그 어떤 유명한 고위인사가 공개방문할 때 실제로 보이는 보안요원들은 그 사람을 호위하기 위하여 배치된 전체 보안무력의 극히 작은 인원에 지나지 않는다. 정보보안역시 사용자전체에게 보이지 말아야 하며 거의 모든 보안틀거리가 막뒤에 숨겨 져 있어야 한다.

정보기술부서들에서 흔히 볼수 있는 공개적인 체계의 환경에서의 투명성이 문제거리로 될수 있다. 여러 판매업체들에서 기술을 받아 리용하면 최고급의 기술을 선택할수도 있고 경쟁력도 조장시키므로 좋은 대안으로 될수 있다. 그러나 중요한것은 여러 업체들에서 구입한 기술형태들의 공개된 표준에 기초하여 서로 흠이 없이 미끈하게 융합되여야 하며 그렇지 않으면 일체화의 노력으로 하여 우점을 다 놓칠수도 있다.

종국적으로 현 정보기술기관들은 《문제점들을 소유》하고 있는 셈이다. 방화벽이나 스마트카드 같은 개별적인 보안《점》제품들을 수많이 살것이 아니라 종합적인 보안기본구조를 실행하는것이 더 좋다고 볼수 있다. 보안기본구조를 이루는 구성요소들은 표준프로그람작성대면부를 리용하여 잘 설계하여 구성요소들호상간 그리고 구성요소들과 현존

정보기술응용기지와 틈이 없이 잘 호상운용되도록 하여야 한다. 제품들은 여러 업체에서 구입할수는 있으나 전반기업의 요구조건들에 부합되는 기본구조에 다 맞아야 한다.

오늘의 전자적인 경제에서 각 기관들은 다른 기관들과 투명하게 서로 통신해야 한다. 이것이 바로 인터네트와 상업적인 폭발력을 가지는 기본요인이다. 세계의 망구성환경은 내부망과 외부망에 긴밀하게 련결되여 있는바 그중에는 인터네트와 호상련결되여 있는것들이 많다. 이로부터 기관들이 호상 망통신을 할수 있는 능력도 높아 진다. 이 모든 망환경에서 바로 자료의 안전이 유지되여야 하는것이다.

다음의 구성요소들이 통합되여 하나의 종합적인 보안체계의 핵심적구조를 이루며 이것들이 바로 비법접근과 도용으로부터 기업집단의 자료들을 보호하게 되여 있다.

보안의 열쇠인 암호화

암호화란 평문으로 된 자료나 문건을 송신자와 소여접수자에게만 알려 진 비밀코드를 리용하여 암호문으로 전환하는 과정을 말한다. 복호화란 그 반대의 과정으로서 암호문을 평문으로 수복하는 과정이다. 문서암호화에 쓰이는 수법들은 수없이 많다. 이것들을 크게 묶어 보면 대칭암호화수법과 비대칭암호화수법으로 갈라 볼수 있다.

자료암호화표준(DES)과 같은 대칭적열쇠구조에서는 송신자와 수신자사이에 공유된 하나의 열쇠를 사용한다. 이 열쇠를 평문에 적용하면 암호문이 나오고 암호문에 적용하면 평문을 만들수 있다. 대칭열쇠방식에서도 송신자와 수신자가 반드시 꼭같은 열쇠를 가져야 한다. 대칭열쇠는 작용은 잘하지만 서로 암호화된 정보를 교환하려는 사람들의 수가 많아 지는 조건에서는 공유규약의 규모설정이 잘되지 않는다.

비대칭열쇠구조에서는 공개열쇠와 비밀열쇠 한쌍을 쓰는데 암호화와 복호화에 각각 다른 열쇠를 쓴다. 공개열쇠암호화기술의 우점은 그 사용자만이 자기비밀열쇠를 쓸수 있으며 사용자가 공개열쇠를 다른 사람에게 준다는것이다. 다른 사람들이 사용자와 통신할 때에 문건을 암호화하려면 공개열쇠를 써야 하며 사용자는 자기의 비밀열쇠로 문건을 암호화한다.

공개열쇠와 비밀열쇠사이에는 반비례적인 수학적관계가 있어 공개열쇠로 암호화한 통신문은 비밀열쇠를 가진 사용자만이 복호화하게 되여 있다. 또한 비밀열쇠를 가진 사용자가 통신문을 암호화한다면 다른 사람들은 그가 보낸 공개열쇠를 가지고 있어야 그것을 복호화할수 있게 되여 있다. 이 특성이 있음으로 하여 열쇠를 사용하자면 문건에 수자식《서명》을 하게 되는것이다.

필수사항인 강력한 암호화

오늘 광범위하게 사용되는 하나의 보안기술(아마 그래서 실제상의 표준이 되였을수도 있는)은 RSA이라는 강력한 공개/비밀열쇠쌍에 전자증명서를 덧붙인 기술이다. 여기서 강력한 암호화라고 할 때 정보가 가치를 가지는 기간이내에 마스기 거의 불가능한 암호

화기술의 사용을 말한다.

강력한 암호화와 약한 암호화를 가르게 된것은 미국정부가 통신문암호화기술의 수출제한조치를 취한데 대해 론쟁이 벌어 진 때부터 시작되였다.

인터네트상에서 전송되는 평문의 전자우편내용과 기타 문서들은 경험이 보여 주는바와 같이 해커들이 다 엿보게 된다. 암호화가 대안이라면 어째서 해커가 남의 열쇠를 추측하여 그 사람의 암호문을 복호할수 없는가. 대부분의 경우에는 시간문제이외에 다른 아무것도 아니다.

해커들이 쓰는 하나의 방법은 평문과 그에 대응되는 암호문표본을 하나 가지고 본문암호화에 쓰인 열쇠를 재건하기 위해 강제적방법으로 임의의 비트렬을 반복적으로 시도해 보는것이다. 그렇기때문에 해커에게 필요한것은 고속콤퓨터나 함께 일할수 있는 콤퓨터들의 망, 평문과 그에 대응되는 암호문이다. 이 강제식공격에 대처하기 위해 암호화열쇠들은 《강해》야 하는것이다.

암호체계의 강도평가

강한 암호화씨나리오에서는 해커의 전략이 고성능콤퓨터자원들을 리용하여 암호화열쇠를 해독하려 하는것으로 본다. 이 해킹공정에 대한 대응책은 해커가 열쇠를 해독하려면 시간이 너무 오래 걸릴만큼 충분히 큰 열쇠를 만드는것이다. 콤퓨터속도가 18개월만에 약 2배로 장성한다는것을 여기서 류의할 필요가 있다. 열쇠의 크기가 너무 커서 해커가 지금에도 미래에도 해독해 내지 못해야 한다. 또한 열쇠를 자주 바꿀 필요도 없지 않는가.

열쇠는 얼마나 커야 하는가. 강력한 암호화는 강제식공격을 저지시킬만큼 충분히 큰 열쇠규모에 기초한 암호화를 의미한다. 따라서 해커들이 강력한 수많은 콤퓨터들을 리용한다 해도 유효시간내에 그 열쇠를 마슬수 없어야 한다. 즉 수년동안에도 복원해 내지 못해야 한다. 열쇠의 크기가 56bit나 이보다 작으면 약하다. 128bit이상의 열쇠규격은 매우 강한것으로 평가된다. 잘 몰라도 오늘의 자료보호에 리용된 열쇠는 최소 75bit길이여야 한다고 생각하면 틀림이 없다. 계산능력이 급속히 발전한다고 볼 때 앞으로 20년동안 정보를 잘 보호하려면 새로 설치하는 체계들에 쓸 열쇠의 길이는 적어도 90bit쯤 길어야 한다.

열쇠관리

열쇠를 안전하게 관리하는것은 극히 중요하며 보안산업에는 이 문제를 해결하는 제품들이 수없이 많다.

해커들의 대부분의 공격은 열쇠자체에 대한 관리를 알아 내기 위한 시도들인데 그것은 강제식공격을 해도 128이상의 bit수를 가진 열쇠를 마스는데는 오랜 시간이 걸리기때문이다.

사용자가 고려해야 할 여러가지 열쇠관리사항들이 있다.

- 사용자는 자기 열쇠들을 매우 안전하고 효률적으로 만들거나 구입하여야 한다.
- 사용자는 자기의 열쇠들을 남들에게 분배해야 한다.
- 타방의 신원에 대한 신뢰를 가지고 타인의 열쇠를 구입해야 한다.

안전한 열쇠관리가 없으면 해커가 열쇠를 마음대로 처리할수 있으며 열쇠사용자로 가장하여 나설수도 있다. 사용자의 공개열쇠의 확실성에 대한 믿음을 주기 위하여 공개 및 비밀열쇠쌍과 함께 수자식인증서라고 하는 형태의 《증명》도 리용한다.

열쇠와 수자식인증서

수자식인증서들은 보안기본구조에서 안전한 구성요소로 되여야 한다. 즉 인증서위조가 불가능해야 하며 불안전한 방법으로 구입하지도 말아야 한다. 또 합법적인 인증서를 비법적인 목적에 사용하지도 말아야 한다. 안전한 기반은 인증서들을 보호하는데 필요하며 인증서들은 또 그것대로 공개열쇠의 확실성을 증명해 준다.

인증서기반의 중요한 기능들중의 하나는 인증서를 취소하는것이다. 누구의 공개열쇠가 도난 혹은 분실되면 그 사람은 자기와 통신하는 사람들에게 알려 주어야 한다. 그들은 그 사람을 위한 그 공개열쇠를 더는 쓰지 말아야 하며 또 효력을 잃은 그 열쇠를 가진 사람에게서 오는 수자식서명을 한 문건도 접수하지 말아야 한다. 이것은 어떤 사람이 신용카드를 분실하든가 혹은 어떤자가 이것을 도적질했을 때와 비슷하다.

열쇠가 만들어 지면 열쇠에는 기한만기날자가 주어 진다. 열쇠란 일정한 시간이 오면 수명이 끝나든가 해야지 그렇지 않으면 마모로 하여 신뢰성이 떨어 질수도 있다. 그런데 여기서 기한만기날자는 해당 환경에서 실시하는 보안방책의 한 부분으로 되므로 심중하게 설정해야 한다. 다른 사용자들에게도 그 만기날자를 알려 주어야 하므로 열쇠들의 기한만기날자를 너무 자주 설정해 놓으면 증명서 및 열쇠관리기반에 부하를 많이 줄수 있게 된다.

수자식서명과 확인

암호화하는것이 통신의 사적비밀보장을 위한것이라면 인증은 어떤것인가 즉 문건을 받아 보는 접수자는 그 문건송신자가 진짜 송신자가 맞는가를 어떻게 확인하는가 또 반대의 경우는? 쌍방을 인증하자면 수자식서명과 확인절차를 결합하여야 한다.

서로 믿는 사이인 제3자에게서 받은 수자식인증서는 개인의 공개열쇠의 신빙성을 보증한다. 이 3자를 인증국(Certificate Authority 즉 CA)이라고 한다. 이 기관은 비전자적인 세계에서 공증소가 하는 일과 비슷한 방식으로 운영된다. 인증서에는 그 개인에 대한 일련의 표준정보가 들어 있게 되며 그 사람의 공개열쇠도 있다. 인증국은 그 사람의 인증서에 수자적방법으로 《서명》을 하여 그의 수자식신원과 함께 그가 가지고 있는 공개열쇠의 유효성도 보증한다.

수자식서명은 전자상업거래대방들에게 법적의의를 가진다. 서명자의 비밀열쇠를 리용하여 쌍방이 다 인정할수 있는 암호화된 서명을 하게 된다. 이 서명은 그 개인의 신원

에 대한 증거로 된다. 즉 오직 비밀열쇠소유자만이 그 무엇을 암호화할수 있으며 그것은 공개열쇠를 가져야만 복호화할수 있다.

인증국이 수자식인증서에 서명해 주는 경우 이 기관에서는 자기의 비밀열쇠를 리용하여 수자식인증서에 보관된 정보 즉 사람의 이름, 인증국이름, 계렬번호 및 인증서유효기간과 같은 정보를 암호화한다. 이 정보를 통보문인증코드(MAC)라고 한다. 보내는 사람과 받는 사람이 다같이 그 인증서에 접근한다. 따라서 MAC정보는 쌍방이 다 확인할수 있는것이다.

서명당사자인 인증국의 공개열쇠만 가지면 누구나 수자식인증서를 확인할수 있다. 어떤 암호문서를 보낼 때 사람들은 신뢰와 확인을 위하여 실제적인 문건교환과는 별도의 단계로서 대방과 인증서를 교환한다.

실례로 제인과 쌤이라는 두 사람사이에 사적인 통보문이 교환되며 호상 확인과정이 있다고 보자. 제인이 암호화된 문서를 쌤에게 보내려면 먼저 쌤의 수자식인증서를 얻어야 하는데 그 인증서에는 CA가 서명한 쌤의 공개열쇠가 들어 있다. 제인은 역시 CA의 공개열쇠를 가지고 CA의 서명을 확인한 다음에야 자기가 가지게 되는 공개열쇠가 정말 쌤의것이라는 확신을 가지게 된다. 그것은 CA의 비밀열쇠가 그 서명에 리용되였기때문이다. 쌤은 제인의 인증서를 받으면 이와 류사한 공정을 재현한다. 물론 대부분의 이러한 공정들은 프로그람적으로 조종되여 사용자가 거의 느끼지 못하며 현 기술수준에서는 그 지연속도가 거의 알리지 않는다.

확인기반

우에서 설명한 두 대방사이의 거래과정은 공개열쇠의 암호화와 확인공정이다. 이것은 간단한 하나의 실례에 지나지 않는다. 그것은 같은 기업내에서도 보안방책에 의하여 부서별로, 지역별로 분리시켜 인증서를 관리함으로써 세밀화된 수준의 보안통제와 책임성문제를 다루어 나가기때문이다.

이 문제에 대한 해결책은 전 세계적으로 오직 하나의 기본인증국이 모든 인증서를 발급하게 하자는것이다. 이러한 운영모형을 오랜 기간 시도하였지만 회사들이 수천수만가지의 인증서에 저마끔 빨리 접근하려고 하기때문에 이 인증국에 병목현상이 생기게 된다. 보안기초에서 중요한 근본문제의 하나는 자기자체의 자원을 자체로 통제하는 능력이다.

인증서관리와 같은 사활적인 책임을 3자에게 떠맡길수는 없는것이다. 그리하여 일부 기관들이 도입해 온 대안이 바로 계층성확인구조를 구축하는것이다. 기관내에 하나의 《고위인증국》을 정하고 거기서 아래수준의 사용자 혹은 부서인증국(UCA)을 확인한다. 고위인증국은 기관의 인증서취소명단(CRL)을 만들어 보존하며 부득이한 경우를 제외하고는 매일매일의 인증서관리사업을 하지 않는다. 이 사업은 사용자인증국이 한다. 기관밖에서는 최고위급의 CA가 임명되는데 이 《방책인증》(PCA)은 모든 고위인증국들을 확인해 두고 기관들사이의 CRL들을 관리하여 기업호상간의 신뢰를 담보해 준다. 마지막으로 세계의 모든 PCA들은 하나의 《인터네트PCA등록국》에 의해 확인되여 확인의 인증기반간의 신뢰를 담보한다.

기업보안기틀의 실현

기업의 정보보안환경을 꾸리는것은 하나의 중요한 복잡한 과제로서 매 기업마다 달라 질수 있다. 이 환경조성사업은 단계별로 해야 하는데 첫단계에서는 보안규정과 그 기본구조의 설계를 해야 한다. 이 두가지는 구조를 잘 짜서 현재와 미래의 요구뿐아니라 예산안작성의 요구도 고려하게 되여야 한다. 또한 고려해야 할것은 기업간요구사항들이다. 즉 전자적인 자료교환에 참여하는 판매업체들, 동업자들, 고객들은 누구인가, 어떤 순위권으로 이 교환을 하겠는가 하는 문제이다.

아래에서는 기업의 안전한 정보기술환경을 구축하는데서 나서는 과업들을 포괄적으로 보려고 한다.

보안검사

보안실행은 권위 있는 회사에 의한 보안검사로 시작되여야 한다. 검사의 역할은 다음과 같다.

- 현 정보기술환경을 기술한다.
- 현재 있는 보안장치의 모든 측면 즉 물리적보안과 함께 쏘프트웨어 및 하드웨어적보안에 대한 모든 측면을 료해한다.
- 발생하였거나 발생할수 있는 보안위반현상들에 대한 구체적이며 기밀적인 분석자료를 마련한다.
- 다른 기관들과 비교할 때 부족되는 점들을 기본으로 현 보안체계에 대한 평가를 진행한다.
- 이전에 일어 난 사고들의 원인에 대한 객관적인 분석을 진행한다.
- 보안하부구조의 개선안들을 권고한다.

기업분석과 보안방책의 개발

다음 단계는 검사결과에 기초하여 기업분석과 함께 심도 있는 보안분석을 해야 한다. 그 다음에야 보안방책이 기업의 실지 요구에 맞게 개발될수 있다. 보안구조는 이 방책에 맞게 개작될수 있을것이다. 이 과정은 다음과 같은 다층적인 공정을 포괄한다.

1. 정보기술기관과 보안인원들사이의 조직적관계의 설정 : 다른 독립적인 보안기관이 있는가, 있다면 정보기술기관에서는 그 방책들이 어떻게 실시되는가, 보안예산은 어떤것이며 자원분배는 어떻게 하는가.
2. 보안 및 정보기술분포모형의 작성 : 본사가 방책을 작성하고 모든 싸이드들에 그 시행을 요구하는가 아니면 원격싸이트들이 자기의 독자적인 정보기술환경에 대한 권한과 책임을 지고 있는가.

3. 기업준위의 보안목적에 대한 료해 : 보호해야 할 기본자원들과 누구로부터 보호해야 하겠는가를 결정한다. 누가 이 자원들을 주로 사용하며 그것으로 무엇을 하는가, 어떤 검사체계가 있으며 물리적고립과 하드웨어/쏘프트웨어에 대한 요구사항들은 어떤것인가.
4. 정보기술판매업체의 영업문제분석 : 여러 판매업체에 비해 하나의 판매업체를 대상하는 문제, 각이한 판매업체에서 제품과 봉사를 구매하는 문제, 숙련 및 지원과 관련한 경험 등
5. 보안강화가 필요한 응용프로그람들, 자료파일들, 봉사기 및 의뢰기체계의 목록작성
6. 현재, 단기 및 장기 정보기술환경에 대한 계획작성 : 영업구성단위들사이에 오가는 자료흐름, 가동환경, 하드웨어, 망의 위상구조, 제3자의 전자적인 호상활동의 요구조건들과 같은 문제의 해결, 공간계획과 물리적보안
7. 높은 수준의 보안구조제기 : 회사의 자료에 대한 정의 및 접근조종을 위한 보안구조의 제기. 실례로 방화벽을 가진 접근조종봉사기, 스마트카드와 단일한 인증, 중앙집권적인증과 같은 계층인증 등
8. 높은 수준의 기업보안방책작성 : 싸이트보안인원, 접근조종, 확인, 기타 기업자원과 보안기반의 호상작용
9. 보안틀거리내에서 그리고 틀거리와 응용프로그람들사이에 존재하는 기본의존관계들을 분석하고 문건화한다.

개발계획작성

일단 높은 급의 보안방책과 틀거리가 구성되면 개발계획은 기초구조를 가지게 된다. 다음 단계에는 그 틀거리구상을 여러가지 과제로 갈라 매 과제들의 규모나 비용을 고려하여 송달과 배치시간표를 짠다.

계획작성단계에는 그 어떤 이렇다할 유일한 방도가 있는것이 아니다. 많은 그룹에서 재능과 자원을 동원하여야 한다. 비용위주이든 복잡성위주이든 실행모형으로 여러가지 대안들을 내놓고 토의하여 선택하는 방법도 있을수 있다.

계획책임자는 이 단계에서 선출해야 한다. 이 책임자는 정보기술개발계획에 대한 넓은 기술적배경지식과 보안실행공정들에 대한 비교적 깊은 지식을 소유해야 한다.

실행모형설정 그 어떤 실행모형의 선택을 권고하기가 힘든것은 정보기술기관들에서 진행되는 여러가지 기타 사업들에 의존되는것이 너무나도 많기때문이다. 실례로 어느 기관이 하나의 중요한 쏘프트웨어계획을 시작하려 한다면 모든 체계들이 공개되여 보안관련부분프로그람들을 갱신하고 기능향상시키는것만큼 철저한 보안계획실행이 선차적인 문제로 나설것이다. 반대로 자원이 이미 파잉할당되였다면 큰 보안관련계획들은 얼마 실행하지 못할것이다.

보안계획을 개시하기 위한 방도는 국부적인 의뢰기/봉사기(군)준위에서 시작하여 싸이트전반의 배치를 거쳐 기업전반에까지 단계별로 전진하는것이다. 매 단계에서 문제점해결은 서로 류사한 방법으로 될수 있다. 실례로 기본인증 및 접근조종체계를 구현하여

개별적장치들과 망주변에 대한 기초적인 보안을 보장하는 방법으로 시작되는것이 가장 좋을것이다.

다음 단계는 망준위에서 중앙집권적봉사를 하는 높은 급의 인증과 접근조종과 함께 사적비밀과 무결성을 보장하는 암호화환경을 구축하는것이다. 마지막으로 망울타리와 망 내부에서 접근조종, 강한 암호화체계, 확인체계, 통표관리, 부인방지 등을 원만히 구현한 정말 강한 보안을 실현하는것이다.

현존체계도 설계형성을 시작하는것이 좋은 설계실천이다. 그 리유는：

- 이 체계가 오늘까지의 기억체계로 바뀌여 지는 기간 수많은 조직구조적인 변화를 거쳐 왔기때문이다.
- 이 체계가 대체로 기업에서 핵심이기때문이다.
- 이 응용체계들을 개조하는데는 부담이 상당히 많이 들기때문에 그 체계를 보안으로 《둘러싸》는것이 더 좋은 전략으로 생각되기때문이다.

보안틀거리개발에는 두가지 기본방법이 있다. 그 하나는 봉사기로부터 시작하여 사업을 바깥쪽으로 나가면서 하는것이다.

이 방법은 일차적인 자료원천에서 보안과 기업을 통합시키는 장점이 있다. 그러나 분권화된 정보기술기관들에서는 의뢰기로부터 안으로 들어 가면서 보안수준을 점차 높이는것이 더 좋은 방도로 될것이다.

의뢰기로부터 안으로 들어 가는 방법에서 리용할수 있는 한가지 수법은 매 의뢰기콤퓨터앞에 스마트카드읽기구동장치들을 설치하여 스마트카드를 통한 현지인증을 하게 하는것이다. 이러한 기능은 후에 더 확장하여 망에 대한 단일개시신호에 의한 접근이나 기타 기능들을 더 추가할수도 있을것이다. 이 방법의 불리한 점은 의뢰기가 추가, 삭제, 판본갱신 등으로 하여 그 수가 계속 변하기때문에 그 수자측정이 곤난하다는것이다. 이 방법으로 하면 보호해야 할 전략적으로 중요한 봉사기자료들은 훔쳐 가지 못할수 있다.

기술기능평가

보안구현모형이 선정되였으므로 이제는 기술기능항목서를 작성하는것이 필요하다. 이 기술기능항목들은 적중한 인원선정과 강습요구수준을 정하는데 필요하다. 기준에 기초한 공개적인 보안장치들을 사용하면 독립적인 환경에서 수많은 사람들을 강습 주어야 할 필요성이 최소화될수 있을것이다.

높은 준위의 작업흐름도를 준비하여 개발팀에 들어 가야 할 해당 단위들을 찾아 내는것이 좋다. 모든 련관단위를 갈라 내고 매 단위의 동원인원들을 찍어야 한다. 공간을 조절하여 설비를 물리적으로 고립시키는것이 필요하면 건물공사도 할수 있다.

이 단계에서 개발팀조직은 정보기술단위와 기타 단위들에서 사람들을 동원하여 할수 있다. 모든 부서들이 이 보안틀거리설계에 다 참여하게 하기 위하여 말단사용자부서들은 개발팀들에 자기 대표들을 파견할수 있다.

규모설정과 자원계획화

설계공정에서 다음으로 중요한것은 개발계획의 규모를 예견하며 자원계획을 잘 짜는것이다. 바로 여기에서 보안틀거리개발계획이 다른 정보기술개발계획들과 맞물림새를 잘 맞추어야 한다. 완성된 정보기술예산안과 동원인원계획을 검토해 보는것도 필요하다. 일부 경우에 개발계획에서 우선권준위도 조절할 필요가 있을것이다. 보안관련세부과제들도 부류별로 묶어 순서를 일관성 있게 잘 정해야 할것이다. 그것은 그 의존성관계가 이미 총 틀거리에서 반영되였기때문이다.

그 어떤 주요정보기술계획에서나 하나의 세부계획에 대해서도 가격 대 성능 비교선택대안들이 제기되고 분석되여야 한다. 이전에 실행된 기업요구 및 보안방책개별분석에서는 공격위험에 대처하여 수많은 자원들을 물리적으로 고립시키는것으로 결론을 찾은것 같다. 이런 경우에는 하드웨어/쏘프트웨어기술에 의한 대안리용으로 나가면 기업전반에 걸쳐 자원을 보다 최량화할수 있으면서도 보안도 더 잘 보장할수 있다.

현지인증방법에는 간단히 사용자의 망주소를 검증하는 방법으로부터 시작하여 정교한 생체검측지표를 리용하는데까지 이르는 등 위력과 비용이 각이한 여러가지 방법들이 있다.

또한 하드웨어와 쏘프트웨어결합을 위해 가격 대 성능 비교대안들을 잘 평가해 보는것도 중요하다. 실례로 보다 강력한 UNIX제품을 쓰는것보다 Windows/NT(r)를 쓰는 방화벽을 구현하여 기능확대출력이 약간 부족한 점을 찾는것이 비용 대 효과면에서 훨씬 낫다고 볼수도 있다. 이것은 정보기술기관안에 있는 기술진의 권고에 의한 결정일것이다.

기술업체의 선정

높은급의 보안방책들과 개발계획이 작성된이상 이제는 제공된 제품을 평가하기 위하여 보안제품판매업체를 분석해야 한다. 현지 정보기술자원을 보충하며 모든 부품들의 대면부를 적절히 맞추기 위해서는 체계통합사업자가 필요할수도 있다. 정보보안제품에 대한 제안의뢰서(RFP)와 자료의뢰서(RFI)들은 상당히 방대하며 따라서 가장 중요한 특성들인 다음의 지표들을 포함하여야 한다.

- **성능, 규모조절.** 보안실행에서 얼마만한 지연을 가져 왔는가, 그리고 사용자와 자원들이 체계에 추가되면 어느정도로 대안이 규모조절될수 있는가.
- **강력성.** 대안이 복잡한 공격에 어느정도로 안전한가.
- **무결성.** 대안이 얼마나 넓고 깊으며 어떤 환경에 그 대안이 가장 적중한가.
- **운용호환성.** 제기된 환경에 대안이 얼마나 잘 융합될수 있는가.
- **지원 및 사용성.** 대안이 얼마나 사용성이 있으며 지원 및 보수특성은 어떤것들인가.

이 다섯가지 기본특성들에 맞게 다음과 같은 포괄적인 질문들을 판매업체의 제품들에 제기해 보아야 판매업체를 평가할수 있으며 해당 정보기술환경에 대한 기타 문제점들도 명백히 해결해 나갈수 있다.

1. 접근조종, 인증, 사적비밀, 무결성 및 부인방지라는 다섯가지 보안기능들중에서 어느것이 제품에 반영되여 있으며 그 작용은 어떠한가.
2. 제품이 방지하게 되여 있는 공격형태들은 어떤것인가.
3. 제품이 가장 잘 들어 맞을 세밀도(network granularity)준위는 어떠한가(즉 의뢰전용, 국부의뢰기/봉사기용, 싸이트용, 기업전반용 및 기업호상용준위)
4. 제품이 가령 어떤 암호화수법을 리용하는가.
5. 그 암호화기술의 원산지가 미국인가, 그렇다면 통보문이 나라들사이에 오갈 때 암호화수준이 《약해 지》는가, 그리고 약해 지면 어느 정도인가.
6. 제품이 보증과 서명을 리용하는가, 구성구조를 서술한다.
7. 누가 보안검사를 진행하였는가, 결과를 제시한다.
8. 어느 표준에 그 제품이 부합되는가, 그리고 사유부가품들은 어느 곳에 추가되였는가.
9. 제품이 《자기 집밖에서》볼 때 어느 3자의 보안관련제품과 호상운용성을 가지는가.
10. 제품이 보안관문, 보안관리프로그람 등과 같은 기관의 현존보안제품들과의 대면상태가 어느정도로 정확한가, 수정해야 할 곳은 어느곳인가.
11. 제품이 수정변경없이 잘 가동할수 있는 제안된 가동환경, 응용프로그람, 도구들은 어떤것들인가.
12. 제품이 모든 지원가동환경들에서 꼭같이 기능을 수행하는가 아니면 다른 지원체계나 훈련이 필요한가.
13. 제품의 사용가능성수준들은 어떤가(례하면 정상적인 유지보수가 필요한가 아니면 매일 24시간 매주 7일 기준의 주기적인 유지보수가 필요한가).
14. 제품관리는 어떻게 하며 제안된 체계나 망관리기반과 쉽게 통합되는가.
15. 제품지원은 판매업체가 제공하는가 아니면 해외조달해야 하는가, 판매업체가 기업에 절실한 환경을 24시간동안 지원하는가.
16. 제품이 부서간, 지역간 그리고 가능하면 기업간 거래를 지원하는가, 얼마나 정확히 지원하는가, 판매업체가 이 기능과 관련한 참조싸이트들을 가지고 있는가, 참조싸이트들에 기초하면 제품들이 어느정도로 사용에 편리한가.
17. 제품들을 단번에 다 배치해야 하겠는가 아니면 단계적으로 도입할것인가, 즉 제품들이 잡탕환경에서 운영되여 례하면 안전한 사용자와 불안전한 사용자사이의 통신이 가능한가.
18. 사용자들과 안전한 자원들이 추가되는 조건에서 대안의 규모조절능력에 대한 정량적인 정보를 제시한다.

실행과 시험

개발계획을 실행하면 계획단계에서는 나타나지 않던 문제점들이 언제나 나타나게 된다. 그렇기때문에 심중히 계획을 작성하며 관리하기 쉽고 명백히 구별된 과제들을 선택하여 개발계획을 짜야 하는것이다.

실행과정이 설계, 개발, 시험 그리고 마지막으로 설치에까지 이르므로 새로운 요구사항들을 이 과정에 도입하지 말아야지 크게 지연할수 있는 가능성이 농후하다. 새로운 요건들은 모았다가 개발계획을 수정할 때 류사한 과정을 거쳐 리용할수 있을것이다.

개발계획의 시험단계가 끝나면 유연하게 이행하기 위해 기업의 기간체계들은 방해하지 않는 국부적인 조종시험을 진행해야 한다. 조종은 통제적인 환경에서 실지 설정에 가능한 한 가깝게 일치되여야 하며 가능한껏 오래 진행하여 그 기술은 물론 보안틀거리개발에 리용된 공정들과 실천들을 검증하게끔 되여야 한다.

결 론

이 장에서는 정보기술보안실행의 기본단계들인 검사, 요구조건분석, 틀거리구성, 개발계획작성, 실행을 보았는데 주로 보안틀거리실행에 유익한 일부 수법들과 고려해야 할 주요문제점들을 중심으로 개괄하였다.

기업보안에 대하여 서술한 이 장에서는 비법접근으로부터 기업정보를 보호하는데서 나서는 보안요구조건들과 구체적인 설계공정 그리고 기업전반의 보안체계실행을 전반적으로 고찰하였다. 이 보안체계를 실현하기 위한 일련의 대안들이 해당 과정에서의 권고안들과 함께 서술되였다. 효과적이며 성과적인 보안실행을 위한 지침도 제시되였다.

기업정보보안은 다음과 같은 다섯가지 측면에서 보아야 한다.

1. 인증
2. 접근조종
3. 사적비밀보존
4. 무결성
5. 부인방지

기업보안체계가 잘되려면 이 기능들을 현존 정보기술환경과 잘 통합시켜야 하며 그 결과 최종체계는 다음의 특성들을 가져야 한다.

- 유연성이 있어 정보기술관리가 보안수준조종을 할수 있는 능력을 가질수 있어야 한다.
- 사용자들에게 줄수 있는 혼란이 최소화되여야 한다.
- 비용효률이 실행에서 높아야 한다.
- 기업망이 계속 늘어 나고 기관적범위와 지리적경계가 계속 뻗어 나가는데 맞게 쓸수 있어야 한다. 보안체계는 기업밖의 기관들에도 운용호환성이 있어야 한다.

제25장. 기업보안정보관리

마툰다 냔차마
애너 윌슨

오늘의 기업환경과 콤퓨터사용환경은 무엇이 신뢰성 있고 무엇이 신뢰성 없는가 하는 전통적인 경계선을 다 모호하게 만들었다. 결과 각 기관들에서는 자기들의 정보를 보호하기 위하여 여러가지 조치들도 취하고 있다. 기관의 망에서 여러 원천을 통하여 나오는 정보들은 보안관리에서 관건적문제로 된다. 이런 정보들이 나오는 원천으로서는 보안장치들(침입탐지체계와 방화벽), 조작체계들, 교환기나 경로기와 같은 망장치 등 수없이 많다.

일반적으로 이 장치들은 매개가 하나의 기능을 수행하여 전반적기업의 요구에 순응하며 결국에는 기업의 보안태세를 확립하는데 기여한다. 또한 이 기술들은 각각 콤퓨터사용환경에서 전반보안관리의 한 부분을 맡고 있는것이다. 총체적으로 이 기구들은 커다란 정보를 생성하는것이다.

우리 앞에 나선 어려운 과업은 이 모든 정보들을 리해하고 콤퓨터사용환경을 보호하는데 유리하게 그리고 전반적기업에 리롭게 관리하는것이다. 이렇게 하기 위해서는 우선 자기의 기술에 정통하며 그 기술의 정보를 어떻게 종합하고 해석하는가, 어느 점에서 사람이 개입해야 하는가를 잘 리해하여야 한다. 이렇게 료해를 잘 하면 기업보안정보관리에 가장 좋은 전략을 가지고 자기식대로 처리해 나갈수 있게 된다.

이 장에서는 종합, 분석, 호상관계를 통하여 기관의 보안태세를 강화하는데 목적을 두고 보안정보를 관리하는데서 나서는 문제점들을 보려고 한다.

이 장에서는 또한 보안관리에 필요한 정보원천들과 그 원천들이 생성하는 정보의 성격에 대하여 해설하려고 한다. 이미 토론된 기술들가운데는 침입탐지체계(IDS), 방화벽, 경로기, 교환기, 조작체계가 있다. 보안관리에서의 그 기본기능, 정보수집방식, 정보분석방법들도 구체적으로 고찰하여 기업전체적인 보안관점을 세운다. 이 정보수집방도들과 정보관리공정에 대한 통지문제를 고찰한다. 이러한 리해에 기초하여 보안정보의 전반적관리를 위한 여러가지 전략들을 투시해 볼수 있다. 또한 보안효과를 높이는 견지에서 보안관리의 문제점들과 이 정보의 관리에서 나서는 난점들을 훑어 볼수 있다. 그 목적은 기술과 사람을 가장 효과적으로 결합시키는 방법을 찾고 기업환경을 안전하게 유지하기 위하여 정보보안일군들을 더 잘 무장시키자는데 있다.

이 장의 자료들은 해당 참고도서들과 련관시켜서 읽어야 한다. 여러가지 망기술과 보안기술에 대하여 서술하면서 필자들은 그에 대한 정보의 성격을 리해하며 이 정보들을 리용하여 기업의 보안을 어떻게 보장하겠는가를 리해시키려는 의도로부터 출발하였다. 이 장이 그러한 기술들에 관한 독자적인 기술참고서로 되게 하기 위하여 구체적인 기술세부들은 깊이 다치지 않았다. 그러나 이 장은 다음과 같은 문제 즉 기업보안정보의 필요성과 그 원천(침입탐지체계, 방화벽, 체계사용기록부, 교환기와 경로기)에 대하여 고찰한다.

기업보안관리와 관련한 일부 전략들은 7편에서 론의된다. 이 전략들에는 종합 및 분석전략들에 대한 방법들도 있다. 이 편에는 또한 취약성자료들을 기업위험과 결부시키는데서 나서는 난점들도 언급한다.

기업보안정보의 원천

장의 이 부분에서는 보안정보의 필요성과 그 원천, 이 정보가 기업보안관리에 어떤 도움을 주는가에 대하여 주로 고찰한다.

보안정보의 필요성

지난 10년간 기술, 전문가, 보안관계정보 등 정보보안문제들이 굉장히 많이 생겨 났다. 일상생활과 상업의 모든 분야에서 콤퓨터와 망들이 노는 중심적인 역할에 의하여 생겨 난 이러한 방대한 문제들은 물리적울타리밖에까지 미치게 되였다. 망통신은 이제 개인이나 기관들의 직접적통제를 벗어 나는 그런 규모로 확대되였다. 또한 모두가 자기의 《령지》에서 통제하려는 노력의 일환으로서 오늘에는 보안기술들이 개발되여 광범위하게 상업화되는 정도에 이르렀다.

한편 망통신은 복잡한 체계들이 각이한 망설비와 장치들로 구성되지 않으면 안되는 결과를 초래하였다. 뒤따라 개발되는 체계에서 정보를 얻어 망과 콤퓨터자원들의 현행관리에 쓴다. 이 정보는 분석되여야 그것이 생산의 환경을 더 잘 리해할수 있을것이다.

전반적으로 보면 보안정보는 기관내의 전체 체계들에서 생산된 총 정보의 한 부분인 것이다. 이러한 보안정보는 보안과 관련된 결심을 채택할 때 매우 중요하다. 이 정보가 없이는 눈이 멀어 가지고도 잘 되겠지 하고 생각하면서 승용차운전대를 잡는것과 같다. 보안체계와 장치에서 생기는 정보의 가치는 콤퓨터사용환경을 어떻게 가장 잘 보호하고 관리하겠는가에 대하여 박식하고도 경제성 있는 선택을 할수 있게 하는데서 유익하다.

검사기록부이든 방화벽기록부이든 침입정보이든 이 모든 정보들은 각이한 측면에서 쓸모 있다.

체계의 활동성격을 결정하기 위하여 체계를 검사할 때 쓰인다.

일상적으로 특히 보안사고일 때 진단프로그람을 실행시키는데 쓰인다.

법정분석에도 필요하며 이것은 사건해결의 중핵을 이룬다. 일반적으로 보안정보는 기업의 보안을 결정하는 중요한 정보이다.

보안정보의 원천

정보보안관리가 효과적으로 되려면 기업전반에 걸치는 각이한 정보쪼각들을 다 필요로 한다. 각이한 원천에서 나오는 이 정보는 기업의 보안정보를 완성하는데 기여한다. 매 쪼각의 정보는 그 내용만큼 유용하다. 이 정보들을 종합하여 전반적인 보안태세를 더 잘

리해할수 있게 된다.

아마 가장 가까운 보안정보원천은 조작체계의 사용기록부이다. 조작체계사용기록부는 아마 보안행정관리가 오늘처럼 자리 잡히기 이전부터 콤퓨터들의 공통적인 특성으로 되여 왔다. 이 기간 체계행정관리자들은 체계기록부를 리용하여 누가 무엇을 언제 어디에서 어떻게 하였는가에 대한 콤퓨터환경을 비교적 구체적으로 관리하게 되였다.

망들사이의 호상련결이 강화됨에 따라 내부망들을 외부망들에 련결하려는 요구가 날을 따라 높아 가고 있다. 신뢰성 없는 망들에 련결하려면 내부망과 외부망들사이의 통신을 통제해야 할 필요가 생긴다. 바로 이런 역할을 하는것이 내부망과 외부망에서 관문의 역할을 수행하는 방화벽이다. 방화벽은 오늘의 망에서 하나의 공통적인 특성이다. 조작체계들이 체계활동에 관한 기록부들을 만들어 내듯이 방화벽들도 관문에서 활동을 추적한다.

조작체계사용기록파일들이 체계상의 활동들을 기록하며 방화벽들이 관문을 통과하는 활동들을 조종하고 기록하는 조건에서 망이 외부공격에 대하여 안전하지 않겠는가고 생각할수도 있다. 이것이 옳은가, 그렇지도 않다. 그것은 어두운 곳에서 모험을 하는자들역시 상당히 령리한자들이기때문이다. 그자들은 이미 구축한 방어체계를 에돌아 《뒤문치기》를 하여 통신규약이나 절차, 응용프로그람이나 조작체계상의 약점들을 교묘히 리용하는 묘리를 알고 있다.

이것은 침입감시체계를 세워 방화벽요새를 보강할 필요성을 강조해 준다. 침입탐지체계(IDS)는 콤퓨터망에 현시된 사건에 대한 정보를 제공한다. IDS는 의심스러운 망활동을 추적하면 그것이 공격시도인가 탐지인가 아니면 성공한 침입인가를 알수 있다. IDS가 제공하는 정보를 보면 내부체계들과 관문에서 놓쳤거나 보지 못했던 약점이나 구멍들을 알수 있다. 이렇게 되면 좋은 기회를 얻어 보안약점과 구멍들이 초래한 부족점들을 강화하거나 메꿀수 있게 된다.

체계들과 방화벽들 그리고 IDS는 서로 각이하나 호상 보안적인 역할을 하여 안전상태를 강화한다. 이 매개의것들은 콤퓨터사용환경에서 하나의 구체적인 역할을 수행한다. 그러나 사실 그것들사이의 경계는 여기에서 설명되는것처럼 그렇게 명확하지는 않을수도 있다. 또한 그것들의 역할이 각이한것만큼 그것들이 생성하는 정보형태, 정보수집방식, 분석 및 해석방식에는 차이가 있다.

보안정보는 망에서 쓰이는 교환기나 경로기에서도 받을수 있다.

경로기나 교환기는 망시설에서 사활적인 역할을 하며 하부구조의 마디들에서도 중요한 요소이다.

각이한 원천으로부터 오는 이 정보들이 종합되면 기업보안에 대한 전체적인 모습이 얻어 지게 된다. 이것들도 종합하여 호상관계가 밝혀 지면 보안관리공정에 도움이 될수 있는 방식과 추세가 산출될수 있다. 실례로 이런 정보를 리용하여 보안사건관리를 향상시키고 배운 경험으로 이와 류사한 사건들의 관리를 잘할수 있으며 사건관리를 사건대응방식이 아니라 사전대책방식으로 전환시킬수 있을것이다.

보안정보를 적중히 활용하고 관리하면 우리의 현 콤퓨터사용환경이 총체적인 보안상《건강》의 처방도 내릴수 있다.

침입탐지체계(IDS)

이 부분에서는 IDS를 중심으로 이것이 무엇이며 기업보안관리에서의 역할은 무엇인가를 설명하려고 한다. IDS는 기업의 건강상태의 맥박을 짚어 보는 도구라고 할수 있다. 이 체계는 변칙적인것들과 이미 알려 진 공격에 토대하여 있을수 있는 공격과 침입을 탐지하고 경보신호를 울린다. 변칙적인것으로 인식하고 어떤 활동을 알려 진 공격과 련결시켜 보는것은 다 제한이 있다.

간단한 소개

IDS는 기업의 보안을 감시하고 시행하는데서 하나의 중요한 역할을 한다. 이 체계들은 흔히 최전방에 배치하여 활동을 감시하고 필요한 행동 즉 해당 활동을 기록하며 경보기나 휴대형호출기를 울리거나 전자우편을 해당 사용자들에게 보내여 주의를 주는 행동을 하게 된다.

IDS는 의심되는 플래그(flag)활동을 탐지하고 해당한 행동을 촉발시킨다. 망상의 통신내용을 감시하거나 특정한 호스트에서의 의심되는 변화들을 감시하든 관계없이 IDS는 기관의 《적극적보안》의 한 구성부분으로 된다.

IDS는 끝없이 제기되는 보안상의 도전들에 직면하게 되므로 계속 갱신되여 가고 있다. 이 도전들에는 IDS탐지를 피하는 해커들의 교묘한 수법들을 따라 가며 대처하는 문제도 포함된다. IDS는 또한 자기를 파괴하려는데 목적을 두는 봉사거부공격과도 싸우지 않으면 안된다.

일반적으로 침입탐지기술은 상대적으로 청소하다. IDS의 구성이 어떤가에 대한 보안전문가들의 의견에는 일련의 차이점은 있으나 기업보안관리에서 IDS가 노는 역할에 대해서는 실질적으로 의견일치가 존재한다. 또한 IDS정보의 분석이 보안관리의 보조수단으로서 필요하다는데 대해서는 의견일치가 있다. 흔히 IDS는 분석을 가하고 행동을 부여하면 기업보안을 개선하는데 도움을 주는 정보의 주되는 원천인것만은 틀림 없다.

리상적인 IDS는 그 기능을 특징 짓는 여러가지 자동화된 구성요소들을 가지고 있는데 그 대표적인것들을 보면 다음과 같다.

- 콤퓨터체계나 망에서 일어 나는 사건들에 대한 정보를 제공하는것,
- 그 정보를 분석하여 보안과정에 도움을 주는것,
- 보안에 예민한 사건정보를 기록하고 보관하며 앞으로 사용하여 개선에 도움을 주는것,
- 그 정보에 대한 행동을 하여 보안을 형성시키는것,
- 우의 모든것들을 결점없이 제때에 시행하는것.

우의 사항들은 모든 보안전문가들에게 있어서 최종적인 IDS의 리상이다. 실지 이러한 체계가 존재하는가 안하는가 하는것은 다른데서 론의할 문제이다.

IDS의 감시방법에는 두가지 기본방식이 있다. 즉 지식기지형탐지와 변칙탐지의 두가지가 있다. 또한 IDS설치방식에도 두가지 기본전략이 있다. 즉 망상설치와 호스트상설치이다. IDS와 사건대응사이에는 밀접한 관계가 있으므로 이것들을 사건대응과 관련시켜 개별적으로 고찰하겠다.

지식기지형침입탐지체계

지식기지형IDS라고 하는 오용탐지식 IDS는 오늘 가장 널리 쓰이는 기술이다. 이러한 IDS에는 표적에 기초하여 이미 알려 진 공격과 취약점들에 대한 지식이 축적되여 있다. 해커들의 묘한 기법이 남긴 공격표적들이 담겨 져 있는 지식기지를 리용하여 이 IDS는 사건형태들과 공격표적들을 비교한다. 공격시도가 탐지되면 IDS는 경보를 울리고 사건을 기록철에 올리고 휴대형호출기에 신호를 보내거나 전자우편을 보낼수 있을것이다.

지식기지형 IDS는 간단하여 실행과 운영이 쉽다. 또한 공격을 신속정확히 탐지하는데 매우 효과적이다. 공격표적들을 끊임없이 갱신하거나 동조하는 방법으로 허위경보들을 줄일수 있다. 그 과정에 보안전문가들은 자기들의 전문기술수준에는 관계없이 사건대응수준을 매우 효과적으로 높일수 있게 된다.

이 오용탐지형IDS에는 하강선도 있을수 있다. 즉 지식기지에 있는 정보가 최신것으로 계속 갱신되여야만 효과가 최상으로 된다. 이미 규제한 규칙이나 공격표적들은 끊임없이 갱신하지 않으면 안된다. 또한 해커의 묘기가 공개된 시간과 해당 공격표적을 얻을수 있는 시간과의 시간차도 있을수 있다.

이것으로 하여 새롭고 탐지하지 못하는 공격이 있을수 있는 공간이 있다.

자기가 《모르는》 수많은 공격형태들에 《눈이 멀게》되는 현상이 생기게 된다. 그것은 특히 IDS의 지식기지의 갱신에서 시간차가 크게 있는 경우에 더욱 그러하다.

변칙탐지(행위형IDS)

행위형IDS라고도 부르는 이 변칙탐지 IDS는 이상적이거나 보기 드문 행위들을 발견해 낼수 있다는 전제하에 동작한다. 호스트나 망상에서 변칙적인 행위들은 정상적이며 합법적인 행동들과 구별될수 있다. 이 차이들을 리용하면 어떤것이 공격인지 알아 낼수 있다.

어떤것이 변칙인가를 결정하기 위해 일정한 기간 호스트 혹은 망상에서의 정상적인 사용자활동을 보여 주는 프로파일들을 구축한다. IDS는 또한 사건자료들을 수집하고 여러가지 계측자료들을 리용함으로써 감시에 포착된 활동이 《정상활동》으로 생각되는것과 비교하여 탈선행위인지 아닌지를 결정한다.

이러한 정상행위를 결정 짓기 위해 다음의 기법들을 일부 혹은 전부 또는 결합하여 쓸수 있다.

- 규칙
- 통계학적측정값
- 림계값

그러나 이 체계도 정상행위로 생각되는 활동의 방식들이 극적으로 변하거나 움직일수 있으므로 허위경보를 낼수 있는 가능성이 있다.

행위형IDS의 주요한 우점은 공격에 대한 특별한 초기지식이 없이도 새로운 공격형태들을 탐지할수 있는것이다. 또한 변칙탐지에서 생성된 정보를 리용하여 지식기지형 IDS에 쓸수 있는 공격방식들을 규정할수 있는 가능성도 있다.

호스트형침입탐지체계

호스트형침입탐지체계는 해당 호스트에 설치하여 거기에서 감시활동을 진행한다. 호스트형IDS는 체계에 따르는 특성에 있다. 호스트형IDS는 체계검열기록부, 체계기록부, 응용프로그람기록부들을 리용하여 IDS정보를 만든다. 체계의 여러가지 기록부들을 리용하면 IDS에서 쓸수 있는정도의 정보가 된다. 해당 조작체계와 관련되는 정보라고 할 때 그 정보의 정확도는 상당히 높은것이다. 그것은 그 조작체계가 자기가 동작하는 호스트의 모든 활동을 정확히 기록하기때문이다.

호스트형침입방지체계는 플래그신호가 있는 사건이 호스트에서 일어 날 때 반응한다. 이러한 행동들로서는 파일변화, 특권위반 혹은 보안적으로 예민한 행동이 해당된다. 이것으로 하여 호스트형IDS는 무결성에 대한 공격을 탐지하는데 매우 효과가 크다. 조작체계의 검사흔적을 리용하면 그 과정에서의 탐지의 불일치를 통하여 트로이목마나 기타 류사한 공격을 예견할수 있다.

호스트형IDS의 또 하나의 우점은 망에서 쓰이는 IDS가 잡지 못하고 스쳐지나보내는 공격들도 탐지할수 있는 능력이다. 정보원천이 어디에서 생성되는가에 따라 호스트형탐지체계는 망전송정보들이 암호화된 환경에서도 동작할수 있다. 교환기술이 망에 리용된 경우에도 이 호스트형침입탐지체계는 영향을 받음이 없이 작용한다.

호스트형 IDS에 일련의 부족점들이 있다. 대개 특정한 체계나 응용프로그람을 위하여 제작되는것으로 하여 이 호스트형IDS는 운용호환성이 높지 못하다. 또한 한 가동환경을 지원하는 IDS가 다른 가동환경은 지원하지 않는 경우도 있다. 체계와 응용프로그람에 각이한 복잡한 환경에서는 매 체계에 서로 다른 호스트형IDS를 설치하려는 생각이 들수도 있다. 이렇게 되면 각이한 IDS를 가진 복잡한 환경이 조성되는데 이것으로 하여 각이한 체계에서 나오는 모든 정보들을 감시하고 관리하는데서 또 문제가 생기기 쉽다.

이러한 부족점에도 불구하고 호스트형IDS는 아직도 중요한 도구로 되고 있다. 그것은 이 호스트에 있는 자원들이 바로 해커들이 많이 노리는 목표이기때문이다. 이것도 역시 하나의 약점이다. 망에서 IDS를 실행시키는 어느 한 호스트가 공격을 받는다고 생각해 보라. 그 호스트에서 첫째가는 타격목표가 어느것이겠는가?

망형침입탐지체계

망형IDS는 설치된 해당 망토막에서 망을 통한 전송흐름들을 감시한다. 이 체계는 매 파케트들을 분석하여 일체 변칙적인것들을 탐지하거나 이미 알려 진 공격표적들과 포착된 파케트를 방식비교하는식으로 탐지한다. 파케트정보에 기초하여 이 IDS는 적대적으로

생각되는 모든것 혹은 적대적인 활동이라고 규제된것과 일치되는 형태들도 찾아 내려고 노력한다.

파케트분석에서는 하나의 난관이 있는데 그것은 여기에서 분석된 정보가 호스트형체계에서만큼은 명백하지 못할수도 있다는 점이다. 여기서는 사실 상당한 정도의 추리를 하여야 관찰된 형태나 탐지된 표적들이 적대활동으로 되는가 안되는가를 판정해 낼수 있다. 그것은 파케트의 물리적원천은 결정할수 있으나 그 원천뒤에 누가 있는지 알수 없기 때문이다.

망형IDS는 비침투성과 스텔스특성을 비롯한 일련의 주요한 장점을 가지고 있다. 자기가 《살고 있는》호스트에 영향을 주는 호스트형IDS들과는 달리 망형IDS의 성능은 체계에 영향을 주지 않는다. 또한 망형 IDS파케트분석은 일정한 형태의 파쇄성공격때에는 호스트형체계에 비하여 더 유리하다.

망형IDS의 주되는 하나의 약점은 망전송량에 비한 규모조절능력이 없는것이다. 전송량이 많은 경우 매 파케트를 검사하는 능력이 이 IDS에서 문제로 나선다. 결과 파케트를 잃어 버리는것이다. 이렇게 파케트를 잃는 량이 많은 경우에는 관리해야 할 IDS정보가 그만큼 적어 지는데 그 정보가 바로 해당 보안에서 치명적인 정보일수도 있지 않는가.

여러가지의 IDS기술들의 장점과 단점을 다 보고 났으니 아마 가장 효과적인 방도는 이 모든것의 적중한 결합이라는것은 명백해 진다.

IDS선택과 배치

IDS의 선택과 배치를 잘하려면 수많은 요인들을 고려해야 한다. 즉

- 그 목적이 무엇인가 즉 호스트형침입탐지인가 아니면 망형침입탐지인가.
- 만일 망형 IDS이라면 대용량전송량에 대비할수 있는 규모조절능력
- 지식기지형인 경우 공격표적의 범위 혹은 정확한 변칙탐지를 수행할수 있는 능력

기타 배치와 관련한 요소들로는 분석되는 정보량, 요구되는 분석도, 감시하려는 침입이나 공격의 중요도 등이다.

IDS를 어디에 배치하겠는가 하는것은 감시하려는 형태의 활동에 따라 다르다. 보안울타리밖(실례로 방화벽밖)에 망형IDS를 배치하면 외부의 공격 그리고 내부로부터 개시되였지만 울타리밖에서 겨누어 조종한 공격들도 감시해 낼수 있다. 반대로 IDS를 보안울타리안에 설치하면 성공한 침입을 발견해 낼수 있다. IDS를 방화벽바깥과 안쪽에 다 설치하면 방화벽규칙(방책)시행을 효과적으로 감시할수 있다. 그것은 이렇게 되면 방화벽바깥에서의 활동과 성공적인 침입사이의 차이를 알수 있기때문이다.

IDS를 배치할 때 그 운영방식 즉 실시간방식(IDS정보가 실시간적으로 분석되는것)인가 아니면 시간격방식(정보가 일정한 시간간격으로 보내져 오프라인 분석되는 방식)인가를 결정하여야 한다. 실시간분석은 여러 원천으로부터 정보가 끊임없이 흘러 들기때문에 IDS에서 즉시적인 행동이 주어 지는것을 의미한다. 시간격 혹은 오프라인분석은 침입관계정보가 앞으로 분석하기 위해 보관된다는것을 의미한다.

이것들중에서 어느것을 선택하겠는가 하는 문제는 IDS정보의 필요성에 기초한다. 즉시적인 행동이 필요하면 실시간방식에 쓰이는것이며 분석이 일없다면 일괄처리방식의 정보수집이 유리할것이다.

사건대응

IDS는 의심쩍은 활동들을 탐지하는데 유리하다. 우에서 설명된바와 같이 IDS는 침입관계정보들을 기록하고 전송한다. 보안관리는 이 정보들을 적중한 형태로 기록하고 분석할것을 요구한다. IDS에 의해 발견되는 그 무엇도 (그것이 공격이든 침입이든 허위경보이든) 모두가 사건으로 되여 분석하고 행동을 촉발시킨다. 사건의 중요성은 그 사건이 주는 위험성에 따라 결정된다.

침입사건이 일어 났다고 생각되는 경우 보안기관은 신속히 대응하고 긴급히 행동하여 침입을 억제하고 그 침입에 의한 피해를 제한하며 피해를 복구하고 전체 체계를 원래의 가동상태로 복구하여야 한다.

일단 사태가 가라앉으면 원인분석을 하여 공격의 성격을 판정하며 이 정보를 리용하여 앞으로 있을수 있는 공격에 대처한 방어망을 개선하는것이 중요하다. 《찾은 교훈》을 보안집행과정에 적용하지 않는다면 그 기관은 앞으로의 공격과 략탈행위에 자신을 내맡기는것이나 갈다.

일반적으로 사건대응과정은 탐지, 대응, 수리, 예방에 기초한 체계적인 과정으로 되여야 한다. IDS는 탐지를 하고 사건에 대하여 경보를 울린다. 사건에 사람이 개입하여 대응하고 수리를 진행하며 얻은 교훈으로 보안을 갱신하도록 한다.

IDS는 공격과 침입에 정확히 대응할수 있는 설정을 잘해야 사건관리를 더 잘할수 있게 된다. 이 대응에는 피동적인것(실례로 사용기록부에 기록하는것)도 있고 능동적인것(실례로 보안관리자에게 경고문을 보내는것)도 있다,

능동대응은 탐지된 침입형태에 따라 자동화된 행동을 하는것이다. 일부 경우 IDS는 공격적인 파케트들을 모두 죽임으로써 공격을 저지시키게 설정해 놓는 경우도 있다. 또한 경로기와 방화벽의 설정을 고쳐 주어 공격자가 사용하는 포구봉사형태, 규약들을 차단시킴으로써 공격자의 접속을 종결시키는 경우도 있다. 또한 발신자주소나 수신자주소에 기초하여 망자료통신을 차단시키기도 하며 필요한 경우 해당 대면부를 통한 모든 접속을 다 차단하기도 한다.

능동대응에서 가장 공격성이 약한 부분은 보안관리자에게 경고를 보내는것이다. 그러면 보안관리자는 공격과 관련한 사용기록부의 정보를 검토한다. 분석해 보면 공격의 성격과 필요한 해당 대응의 성격을 인차 알수 있다. 이 분석결과에 기초하여 이 IDS의 민감도를 조절하여 대응필요성에 부합되게 할수 있을것이다.

이렇게 하자면 체계의 민감도를 높여 보다 넓은 범위의 정보를 수집하여야 공격이 실지 일어 났는가를 정확히 진단할수 있다. 이 정보를 수집하면 후에도 공격을 조사할수 있으며 필요하면 법적증거로도 될수 있다.

공격에 대응하는 다른 방도들도 있는데 그중 하나는 맞받아 싸우는것이다. 공격자에 대한 정보수집, 공격자에 대한 공격을 가하는것 등은 그 단적인 실례들이다. 일부 사람들

에게 상당히 매력 있게 보이지만 이런 형태의 수법은 오직 공격자에 대한 정보수집의 범위에서만 리용되여야 한다.

공격이라고 생각되는것에 대하여 적극적으로 공격을 가하는것은 그 잠재적인 위험성이 크다. 실례로 통신발신자의 IP가 위조되였다고 가정하면 마지막공격지는 공격원천이 아니라 공격의 발판으로 된셈이다. 또한 이것은 법적인 문제도 안고 있다. 그렇기때문에 이쯤알고 전문가들은 자기의 법적경계선을 명백히 알고 그 경계를 넘지 않도록 주의해야 할것이다.

오늘날의 상업화된 대부분의 IDS들은 공격정보를 기록부에 기록하고 경보를 울리는 피동대응식체계들이다. 이것은 항상 사람이 개입하여 IDS정보에 대응할것을 요구하는 체계이다. 이런것들은 경보신호, 통지신호, SNMP(단순망관리규약)통보문의 형태이다. 경보나 통지는 공격이 탐지되였을 때 발생하는데 콤퓨터화면에 하나의 창으로 튀여 나오거나 전자우편통보문으로 보내여 지든가 아니면 이동전화나 휴대형호출기에 경고신호를 보내는 식으로 발신된다. 일부 업체의 IDS들은 사용자에게 일정한 정도의 선택점을 주어 의심되는 전송자료들을 《적극적으로 죽일수 있게》한다.

망으로 경보정보를 내보낼 때 많은 체계들은 SNMP통보문들을 리용하여 망관리체계에 경고를 내보낸다. 현재 하나의 조종탁을 통하여 보안사건들을 공고화하고 관리하는 보안관리체계가 시장실현되고 있는것으로 생각된다. 이러한 체계의 우점은 그 총체성성격이므로 망하부구조전반이 공격대응에 중요한 역할을 수행할수 있게 하는것이다. 널리 인정된 많은 망관리체계들이 현재 이 요구를 충족시키기 위하여 자기들의 체계들에 보안전용 모듈들을 합장하고 있다.

IDS기술이 충분한 보안능력이 있는가

보안관리에서 IDS의 역할과 사건대응의 역할을 다 리해한바와 같이 IDS의 기술은 그정도가 전부이다. 즉 경보를 울리고 보안관련사건을 기록하며 불쾌한 전송자료들은 일정한정도로 적극적으로 살상하는 능력이다. 기업전반에 걸쳐 IDS가 생성하는 정보들을 리용하면 보안사업개선을 위한 권위 있는 결정들을 채택할수 있다.

아무리 정교한 최신 IDS를 가지고 있다 해도 전문가들의 사건분석이 있어야 대응 및 관리공정을 향상시킬수 있는 사활적인 자료를 쥘수 있다. 경보울린사건이 일단 포착되고 위험사건으로 판정되면 사건대응팀은 재빨리 대응하여 그 사건이 더 번져 가지 않으며 망과 체계들이 그 어떤 있을수 있는 피해를 받지 않도록 하여야 한다. 이 시점에서 법정토론술의 역할이 발휘된다. 토론술전문가들은 사고의 원인과 결과를 판정하기 위한 구체적인 분석을 진행한다. 이 토론된 분석의 결과자료들을 가지면 대답을 찾는데 필요한 정보를 얻을수 있다. 이 정보를 가지고 적대공격, 봉사거부공격, 정보기술람용 등과 같은 여러가지 부류로 분류하면 통계적자료도 얻을수 있으므로 앞으로의 사고처리대응을 보다 높은 수준에서 할수 있게 될것이다.

마지막으로 이 정보를 리용하여 분석과정에서 포착된 약점들을 처리할 필요도 있을것이다. 이러한 부족점들은 체계와 망에 있는 기술적취약성이나 제한성일수도 있고 방책이나 절차와 같은 행정통제사업일수도 있다. 앞으로 있을수 있는 사건들을 미리 잘 접종

함으로써 재발의 위험성을 막아야 할것이다. 한가지 문제점이 있다. 지난번의 감염에서 교훈을 찾지 않아 동일한 비루스와 싸우지 않으면 안되는 보안전문가들이 얼마나 되는가. 일이 번져 진 다음에 하는 일들도 보안태세향상에 도움을 주며 찾은 교훈을 분간하여 보안의식을 높이는데 큰 역할을 할것이다.

기타 IDS관리의 문제점으로서는 IDS를 갱신하고 동조시켜 최신공격들을 잡아낼뿐아니라 허위경보들도 려과하도록 하는것이다. 모든 체계에서 그러한것처럼 IDS를 항시적으로 유지보수해야 IDS가 생성하는 정보가 실용성 있게 된다.

방화벽의 형태와 보안실시에서 노는 그 역할

이 부분에서는 방화벽들과 정보보호에서 그것이 노는 역할을 각이한 형태의 방화벽과 보안관리에서 그 우단점과 결부하여 개괄한다.

소개

방화벽은 지역간의 접근을 조절함으로써 서로 다른 망지역간에 보호를 보장하는 도구이다. 일반적으로 방화벽은 해당 규칙에 토대하여 특정한 봉사형태나 응용을 려과하며 망경간들사이의 접근을 조종함으로써 정보를 보호해준다.

방화벽은 다음과 같은 주요장점을 가지고 있다.

- 공통의 접근점을 통하여 보안을 공고화하는 능력. 방화벽이 없는 경우에 보안능력은 오직 해당 호스트나 망장치들에 의하여 수행된다. 이렇게 공고화하면 보호되는 경간들에서 중앙집권적인 접근관리를 실현할수 있다.
- 단일접근점으로서 방화벽은 망전송내용을 기록하는 점으로도 된다. 방화벽작업기록철은 방화벽을 통과하는 전송자들의 성격에 대한 정보를 제공하므로 그 내용은 다양하다. 이러한 전송내용은 침입과 관련한것일수도 있으므로 이것을 분석하면 해당 보안위험사항들의 성격을 료해할수 있다.
- 방화벽뒤에 있는 내부망의 성격을 감추는 능력(이것은 사적비밀보장에 큰 도움이 된다).
- 외부의 략탈위험을 받지 않고도 방화벽뒤에서 봉사를 제공할수 있는 능력.

핵심적인 보안기능을 수행하지만 방화벽은 기관의 보안을 담보하지는 못한다. 보안이 효과적인것으로 되는가 하는것은 해당 보안공정과 절차들을 비롯하여 보안이 어떻게 관리되는가에 달려 있다. 또한 방화벽의 설정과 관리를 담보할수 있는 준비된 인원들이 있어야 한다.

전반적인 방화벽이 기관의 보안을 향상시키는데 도움을 주지만 여기에는 일련의 단점이 있다. 이러한 결함들로서는 일부 종류의 봉사와 호스트들이 망접속을 제대로 하지

못하여 유일한 《실패점》으로 되는 현상을 대표적으로 볼수 있다.

방화벽설정에는 주로 두가지 방법이 있다. 즉

- 거절하게끔 설정된것들만 제외하고 모든것(파케트와 봉사)을 다 허용하는것
- 허용하게끔 설정된것들만 제외하고 모든것(파케트와 봉사)을 다 거절하는것

《모든것을 다 허용하는》방책은 조종적접근에 대하여 일정하게 제한시키려는 요구와 어긋난다. 표준적으로 대부분의 방화벽들은 《허용하게끔 설정된것들만 제외하고 모든것을 다 거절하는》방책을 실시한다.

방화벽의 형태

파케트려과장치. 파케트를 려과하는 방화벽들은 IP층에서 기능을 수행하여 파케트형태를 검열함으로써 보안방책에서 허용된것들만 통과시키고 기타는 일체 무시하는 작용을 한다. 파케트를 려과한다는것은 파케트형태, 발신자 1P주소와 수신자 IP주소 혹은 발신자 TCP/UDP포구들에 기초한 려과라는것을 의미한다. 대표적으로 보면 파케트려과는 경로기로 수행한다.

파케트려과의 기본장점은 상대적으로 값눅으면서도 높은 준위의 성능으로 보안을 보장한다는것이다. 또한 그것을 사용하는것이 사용자들에게는 항상 투명하다는것이다.

그러나 파케트려과는 약점도 있는바 그것은 다음과 같다.

- 설정하기가 보다 힘 들며 그 설정을 확인하는것은 더욱 힘들다. 설정오유의 가능성이 높으면 보안상 구멍의 위험성도 높아 진다.
- 사용자준위의 인증은 지원하지 않으며 시각에 기초한 접근도 허용하지 않는다.
- 다만 제한된 검사능력만 있으며 국부망을 외부세계로부터 숨기는 능력은 없다.
- 망층보다 더 높은 규약을 겨눈 공격에는 취약하다.

응용프로그람관문. 응용프로그람관문들은 응용층에서 작용하여 파케트려과보다 더 세밀하게 전송내용을 조사한다. 해당 대리자가 있는 봉사에 한해서만 통과를 허용한다. 대리자봉사들은 또 그것대로 오직 믿음직한 봉사들만 방화벽으로 통과허용되게끔 설정된다. 새로운 종류의 봉사들은 자기들의 대리자가 규정되여야 비로소 통과허용을 받을수 있다.

일반적으로 응용프로그람관문들은 파케트를 려과하는 방화벽보다 더 안전하다.

응용프로그람관문들에 토대하는 방화벽의 주요우점들은 다음과 같다.

- 내부망이 밖에서 《보이지》않으므로 정보숨기기를 잘할수 있다. 실지 응용프로그람관문들은 내부망구조를 숨기는 기능이 있다.
- 인증과 기록을 할수 있으며 내부적인 우편전달을 중앙집권화할수 있게 한다.
- 검사능력이 있어 발신자주소와 도착지주소, 넘겨 진 정보의 크기, 시작 및 끝시간, 사용자신원과 같은 정보의 추적이 가능하다.

● 하나의 봉사내에서 일련의 명령들에 대한 려과를 정교하게 시행시킬수도 있다. 례하면 FTP응용프로그람관문에는 Put와 get명령을 려과하는 능력이 있다.

응용프로그람관문의 결정은 의뢰기와 봉사기의 련결이 두 단계적인 공정이라는것이다. 그 관문들의 작용내용은 사용자에게 투명치 않다. 또한 전송내용의 검사범위때문에 응용프로그람관문들은 대체로 파케트려과보다 속도가 느리다.

방화벽관리의 문제점들

보안실천이 잘되자면 방화벽활동이 끊임없이 기록되여야 한다. 안전한 망을 통하여 안팎으로 나드는 모든 전송자료들이 방화벽을 거치며 기록부의 정보를 보고도 전송의 성격, 사용패턴, 수신지와 발신지 등에 대하여 상당한 정도로 인식이 서게 된다. 또한 기록부정보의 분석을 통하여 보안계획작성뿐아니라 망리용에까지 이르는 수많은 귀중한 통계학적자료들도 될수 있다.

필요하다면 방화벽이 일정한 정도의 침입탐지기능도 가질수 있다. 적중한 경보장치로 설정을 잘해 놓으면 방화벽은 자기와 망이 공격이나 탐색당하는가 아닌가에 대한 훌륭한 정보제공원천으로 될수 있다. 이것은 IDS와 함께 쓰는 경우 훌륭한 보안적역할을 놀수 있을것이다.

망용도통계자료와 탐색의 증거는 여러 목적에 쓰일수 있다. 1차적인 중요성을 가지는것이 바로 방화벽이 외부의 공격에 견딜수 있는가 없는가 하는 문제의 분석과 방화벽에 있는 통제기능들의 강력한 보호기능을 수행하는가 못하는가를 결정하는것이다.

망용도통계자료들은 망요구사항연구와 위험분석활동에서 주요한 입력자료로 된다. 공격 및 침습에 대한 연구의 최신수법들에는 《꿀통》수법이라는것도 있는데 이 수법은 전송방식, 있을수 있는 공격, 이러한 공격들의 성격 등을 연구한다. 여기에서는 이미 알려 진 취약점들을 담은 《꿀통》을 배치하여 침입시도, 그 성격, 성공여부, 공격발원지 등을 잡아 낸다. 이 꿀통식분석수법으로는 공격자들의 공격동기, 해당 공격형태의 성공률 등을 결정해 낼수 있다.

방화벽보안이 충분한가.

방화벽을 설치하고 설정한 후에는 나앉아서 방화벽의 정보가 다 안전하다고 만족감을 가지는 기관들이 허다하다. 실생활에서 방화벽은 하나의 큰 정문과 류사하여 대부분의 침입자들이 구멍만 찾아 내면 들어 오기 쉬운것이나 같다. 실지 침입자가 에돌아 들어 오거나 불법리용하여 방화벽을 뚫고 들어 와 내부망에 접근할수 있는 방도는 많다. 이런것들로는 규약 혹은 응용프로그람특유의 약점을 교묘하게 리용하는것과 내부망의 안팎을 통하는 예비적인 통로가 있는 방화벽을 에돌아 가는것 등이 있다.

현실적으로 최상의 보안을 담보하는 문제들이란 다름 아닌 공정들과 사람들 그리고 기술에 귀착된다. 기술도 좋다. 그러나 그 기술을 관리할 사람이 있어야 한다. 그리고 보안과 보안을 실시하는 사람을 관리해야 할 공정도 있어야 한다.

주요 공정들은 다음과 같다.

- 쏘프트웨어의 시간갱신과 판본갱신의 적용
- 보충프로그람의 구입과 적용
- 방화벽을 잘 설정하여 기록철들을 묶고 그 정보를 수집하는것
- 보안에 예민한 문제들에 대한 기록정보의 후열
- 기록정보를 망의 다른 보안장치의 정보들과 호상 련결시켜 보는것
- 보안정보에서 밝혀 진 조사결과들을 결정하고 그 결과들에 대응한 행동을 취하는것
- 이 주기들을 반복하는것

조작체계기록파일

여기서는 조작체계기록철(log)이란 무엇이며 왜 필요한가 하는것, 기록철정보수집방법, 체계기록철관리전략, 기록철정보관리에서의 난점들, 체계안전에 주는 영향들을 종합적으로 보여 준다.

소개

조작체계기록철은 체계정보의 수집과 분석에서 하나의 중요하고도 유용한 도구이다. 이 기록철은 체계활동과 관련한 귀중하고도 세부적인 정보를 제공해 준다. 체계기록철은 사용자, 보안, 체계관련사항, 응용프로그람관련사항들을 비롯한 일정한 활동정보를 기록하는 여러가지의 부류로 나누어 진다.

이것들은 진행중인 조작과정을 지원하며 체계의 활동흔적을 제공해 준다. 이것을 리용하여 체계가 손상이 갔는가를 결정할수 있게 해주며 범죄활동이 있는 경우 법정에서 중요한 증거문건으로 된다.

기록철의 류형, 용도, 우점들

조작체계를 검사하면 체계활동, 응용프로그람의 활동, 사용자활동에 관한 정보가 모두 기록철에 기록된다. 조작체계에 따라 여러가지 이름으로 기능을 수행하나 매 기록철은 자기 부류에 해당한 활동을 기록하는 책임을 가지고 있다. 체계는 활동기록을 두가지 방법으로 한다. 즉 사건형기록과 타건형기록(타건감시)이 있다.

사건형기록은 체계, 응용프로그람 혹은 사용자의 활동과 관련한 정보를 담는다. 그리하여 사건이 일어 나면 사건에 대하여, 그 사건과 관련한 사용자 ID, 그 사건에 어떤 프로그람이 사용되였는가 하는것과 그리고 그 최종결과까지 알려 준다.

타건감시는 특수한 형태의 체계기록철이라고 볼수 있다. 이것을 둘러 싸고 법적문제

까지 생길수 있다. 사용하기전에 이것을 잘 알아야 한다. 이런 검사방식을 쓰면 사용자가 건반을 칠 때마다 기록된다. 때로는 건반칠 때의 콤퓨터의 반응도 기록된다. 이런 체계기록은 침입자가 콤퓨터를 파괴했을 때 그것을 수리하는 체계사용자에게 매우 유용하다. 체계기록정보를 리용하여 체계의 성능도 감시할수 있다.

구동프로그람적재, 공정, 봉사시작, 처리률과 같은 활동은 체계관리자가 체계를 세밀조절할수 있는 귀중한 정보이다. 또한 이 기록철들은 체계접근에 대한 정보와 어떤 프로그람들을 자극시켰는가에 대한 정보를 잡을수 있다.

사용자활동과 관련되는 사건들을 모으면 개인의 책임소재가 성립되며 성공하였거나 성공하지 못한 인증시도에 대한 기록도 알수 있다. 이 기록철을 보면 사용자가 시행시킨 명령들에 대한 정보, 어떤 자원이나 파일에 접근하였는가 하는것도 알수 있다. 보충적인 세밀도가 필요하면 파일읽기나 변경과 같은 응용프로그람내의 세부활동도 기록할수 있다. 응용프로그람기록부는 응용프로그람내에 결함이 있는가 또한 어떤 응용프로그람전용보안규칙들이 위반되였는가를 결정하는데 쓰이기도 한다.

이 검사기록부들의 좋은 점을 말하자면 끝이 없다. 사용자관계사건들을 기록함으로써 개인의 책임소재를 성립시킬수 있을뿐아니라 사용자들로 하여금 자기들의 활동이 날날이 기록된다는것을 알게 하여 금지된 령역에 감히 들어 가지 못하도록 할수도 있을것이다. 체계기록철들은 접근조종체계와 침입방지체계와 같은 다른 보안체계들과 협동하여 사건들에 대한 보다 심화된 분석을 가할수도 있다. 가동이 중지되는 경우 기록철을 잘 리용하면 그 사건을 유발시킨 활동을 찾아 내고 더 나아가서 그 근원을 밝혀 낼수도 있을것이다.

물론 이 기록철이 리용성이 높자면 기록들이 모두 정확하며 그에 대한 해당한 조종을 강화하게끔 되여야 한다. 또한 그 기록철의 무결성이 보호되여야 하며 기록철에 기록된 약점이나 결점이 잘못된 대상에 알려 지는 경우 그 정보의 로출은 큰 부정적후과를 가져 올것이다. 많은 경우 조작체계기록철 즉 검사기록철은 침입자나 내부사람들의 공격대상으로 될수 있다.

관리에서의 난점들과 영향

조작체계기록파일들은 의심할바없이 우리 체계들의 매우 중요한 부분이다. 그러나 수집되는 정보량은 효과적으로 관리하기 매우 힘들다. 기록파일에 담겨 진 정보들은 거기에 담겨 진 비정상행위들을 정기적으로 검열하지 않는다면 실지 무용지물이 되고 만다. 이것은 한사람은 더 말할것도 없고 여러 사람이 모여 검열하기에는 아름찬 과업인것이다. 검열자들이 정보를 정확히 해석하고 해당 행동을 취하려면 어떤 비정상적인 배척사건을 찾고 있는가를 잘 알아야 한다. 기록된 사건들중에서 비정상행위로 되는 추세, 형태, 변종들을 찍어 밝혀 낼수 있게 되여야 한다. 매일 기록파일에 기록되는 정보의 량을 타산해 보라. 이 정보를 효과적으로 관리할 책임을 보안전문가 한사람에게 맡긴다면 그 힘든 정보는 너무나도 뻔하다. 한사람 혹은 한 그룹이 전문으로 해야 할 일량이 쉽게 될것이다.

만일 이 방대한 량의 정보관리로 하여 보안전문가가 쓰러 져 휴가받으면 정보의 보관과 가공에 드는 비용은 더 말할것도 없고 이 정보수집기간 체계에 어떤 영향이 미치겠

는가 하는것을 상상하기 어렵지 않다.

다행히도 이 모든 정보를 계속 관리할수 있는 분석도구들도 있다. 검사정리도구들을 쓰면 정상운영과 관련된 활동들과 같은 보안상 후과가 적은 사건들을 제거하여 남은 정보를 중시함으로써 자료량을 줄일수 있을것이다. 침입탐지체계기능들과 류사한 경향/변화탐지도구들과 공격표적탐지체계들은 가능한 모든 원자료들에서 유용정보를 추출해 낼것이다.

결론

조작체계기록파일들은 기관의 체계들과 자원들에 대한 기술적인 보관관리에서 귀중한 수많은 유효정보들을 그 값을 물지 않고 제공할수 있다. 이러한 정보들을 값 있게 관리하자면 시간, 콤퓨터자원을 다 바쳐 그리고 고심분투하여 나가야 할것이다.

기타문제 : 경로기와 교환기

경로기와 교환기는 기업망에서 실로 중요한 역할을 논다. 경로기는 서로 다른 망토막들을 련결시키며 한 토막에서 다른 토막에로의 전송흐름을 경로조정해 준다. 망에서 결정적인 지점들에 《앉아 있다》고 말할수 있다. 경로기는 망쪼각들을 서로 붙이는 풀이라고 볼수 있다. 가장 간단한 망에서조차 이것은 간단한 작업이 아니다.

경로기처럼 교환기들도 망에서 결정적인 요소들이다. 교환기는 하나의 망에 해당된 전송흐름을 분류하여 망토막들을 갈라 준다. 교환기와 경로기는 실질적인 콤퓨터의 능력을 가진 일정하게 복잡한 기구로 변화되여 가고 있다. 또한 교환기와 경로기가 망기능에서 노는 결정적인 역할로 하여 보안에 주는 영향역시 결정적이다. 경로기들은 고도로 전문화된 콤퓨터가동환경으로 변화되여 고도의 유연성과 복잡성을 가지게 되였다. 이러한 복잡성으로 하여 취약성이 생겨 나고 결과 공격도 자주 받게 되는것이다.

경로기, 교환기와 관련된 문제점들은 다음과 같다.

- **접근** 그 장치에 누가 어떤 접근를 하였는가.
- **설정** 설정을 어떻게 하여야 장치의 보안이 담보되는가.
- **성능** 배치된후 소여요구사항들을 만족시키기 위하여 얼마나 잘 동작하는가.

우의 사항들에 대한 정보를 추적하여 망장치들과 그 성능들의 《건강》을 확인하는것은 흥미 있다. 장치건강상태를 확인한다는것은 장치가 원래의 목적에 기초하여 기능을 계속 수행하고 있는가를 확인한다는것을 의미한다. 장치들의 변화와 성능을 주시할뿐아니라 그 변화들이 합법적으로 승인받은것인가와 그 장치의 보안에 주는 영향을 정확히 알아야 한다.

경로기와 교환기를 관리하는 문제는 방화벽과 IDS와 같은 망장치를 관리하는 문제

와 류사하다. 방화벽이나 IDS와 같이 교환기와 경로기들은 응당한 관심을 돌릴것을 요구한다. 즉 이상한 행동들을 사용기록파일에 기록하여 필요한 경우 경보를 울리며 장치를 보호하기 위하여 기록파일들에 기록된 활동들을 정상적으로 검열해 보아야 한다.

방화벽과 IDS를 사용할 때처럼 사용자들은 경로기와 교환기들이 기정설정값으로 설치하지 않도록 하여야 하며 장치시간갱신과 추가보충과정이 반드시 있게끔 하여야 한다.

표준적으로 교환기와 경로기는 내부망에서 쓰인다. 이런데로부터 많은 사람들은 교환기와 경로기가 기관울타리에 설치하는 장치보다 낮은 수준의 보호밖에 제공하지 못하는것으로 생각하군 한다. 사실상 울타리가 안전하면 그 내부의 보호수준이 반드시 낮겠구나 하고 생각하는 사람들이 없지 않다. 이것은 대부분의 공격사건의 원천이 내부망이라고 생각하는 그릇된 보안관념에서 출발한것이다. 더우기 공격이 성공하는 경우 침입자는 내부망장치들의 보호가 충분하다고 해도 제마음대로 만들어 놓을것이다.

더 있다. 망의 내부와 외부사이의 경계가 계속 흐려 지고 있다. 표준적으로 한 기업이 가지고 있는 망은 인트라네트, 엑스트라네트, 내부망과 인터네트로 구성되여 있다. 가장 약한 고리를 쳐야 보안사슬이 끊기게 된다. 기업대상자와 그 기업을 련결시키는 경로기나 교환기가 가장 약한 고리로 될수 있다. 그러므로 이 장치들을 안전하게 관리하는데 많은 관심을 돌려야 한다.

경로기나 교환기에서 얻은 보안정보는 반드시 기업보안정보총체의 한 부분으로 되여야 한다. 그렇게 하여야 기업보안태세에 대한 전면적인 모습을 그릴수 있을것이다.

기업정보관리전략

기업정보를 관리한다는것은 기업보안 및 위험관리자들에게 상당한 애로를 주고 있다. 그 애로에는 수없이 많은 망장치들이 생성하는 방대한 량의 정보, 그 정보의 분석, 보안사건과의 호상관계수립, 기술적위험과 기업위험과의 호상관계의 설정 등이 속한다. 또한 보안 및 위험관리자들은 이 보안관계활동들을 끊임없이 진행하여야 기관의 보안상태를 손금보듯 알수 있으며 그 상태의 개선방도를 찾을수 있게 된다.

기업보안태세를 잘 파악하려면 각이한 원천에서 나오는 정보들을 의미별로 종합하고 호상 련결시켜야 한다. 그 다음에 그것들을 분석해 보면 그 정보에서 특징적인 방식, 경향, 성능지표들을 알수 있다.

방식들을 보면 체계리용률의 측면들을 알수 있게 된다. 이 측면들은 또 기업보안개발계획 및 유지관리공정의 성격을 반영하게 된다. 한편 경향을 보면 일정한 기간내에 보안의 여러 측면에서의 변화를 알수 있다. 이것들은 다 실현된 개선항목들을 보여 주며 또한 개선해야 할 문제성 있는 분야들을 가리켜 준다. 성능지표들과 방식들은 또한 원인분석과 문제해결에도 도움을 준다.

보안 및 위험관리에서 나서는 가장 어려운 과업은 기업내의 각이한 망장치들에서 수집된 정보를 분석하는것인데 그 장치들은 다 각이하나 호상 보충완성하는 보안기능들을 발휘한다. 실례로 방화벽, 침입탐지체계, 체계기록파일에서 오는 정보들은 보안상 서로

보완적인 성격을 띠고 있다. 이 각이한 원천의 정보들을 정확한 련관관계로 맺어 준다는 것은 아직은 주요애로들중의 하나이다.

수집된 방대한 량의 정보처리문제를 제쳐 놓고 보더라도 그 분석과정을 쉽게 할수 있는 특수한 분석기법이 반드시 있어야 한다. 이 기법들은 변칙, 호상관계, 알려 진 로출과의 관계, 경향 그리고 사용자자료 등에 기초한다. 이 기법들은 보안정보를 려과 및 수집하여 대량의 자료요소들을 결심책택에 필요한 유용정보로 전환시켜 준다.

일반적으로 문제의 범위는 기술, 공정, 사람 그리고 기업이다. 이 문제들은 보안태세향상에 유용한 정보를 위한 이러한 총체속에서 고찰되여야 할 문제이다.

이 부분의 뒤에서는 보안정보관리문제들과 보안정보관리의 난점타결안들을 총괄적으로 보기로 한다. 여기에서 취급되는 실천적문제들이 보안태세향상에 유익하지만 이 모든 것을 다 구현하여야 기업보안전반에 개선을 가져 올수 있다. 정보보안실험자들은 보안이란 사회적 및 기술적인 측면을 다 포함한다고 본다. 이런것으로 하여 기관내의 관례와 기준 특히 자체개선을 추동하는 관례와 기준들은 기업보안향상에서 핵심으로 된다.

보안자료수집과 기록부관리문제점

기업전반에서 보안관계정보의 수집, 보관, 분석은 기업보안의 경향성을 료해하는데서 사활적이다. 관리자들은 기업운영에 도움이 되게끔 이 방대한 량의 정보를 관리할수 있는 방도들을 찾아야 한다. 구태여 찍어 말하면 기술적취약성자료를 기업위험으로 어떻게 해석할수 있겠는가.

려과를 잘 하지 못하여 기업에 절실한 정보만 골라 내지 못한다면 방대한 정보량에 목이 멜수 있는 위험요소도 있다. 보안관계정보려과장치를 선택하는 문제는 경험에서 나오며 어떤 정보환경인가에도 달려 있다.

보안필수정보들은 보존하고 불필요한 정보는 다 제거하는 식의 정보수집에도 난점이 아직 남아 있다. 실례로 대부분의 침입탐지체계들은 IDS의 수감부설정에 대하여 수많은 허위긍정을 하는 현상이 있다. 사실상 그 탐지체계들이 생성하는 많은 정보들은 《백색소음》으로 분류될수 있으며 보안관리에는 의의가 그닥 없다. 보안관리자들에게는 적중한 려과기를 설계함으로써 백색소음를 려과하여 정보관리의 부담을 덜어 주어야 할 과업이 나선다.

보안정보수집과 관련하여 나서는 기초적인 다른 문제들도 있다. 기록철정보를 보관한 충분한 보관공간의 확보, 수집정보들의 중앙기록부수집호스트에로 주기적으로 전달하는 문제들이 그런 문제들이다. 많은 경우 기록철자료수집에 대한 충분한 계획이 없이 개발계획이 실행되군 한다. 이것은 사고가 발생할 때 원인분석을 극히 어렵게 한다.

기타 기록파일관리문제들로서는 기록철정보검열을 들수 있다. 많은 기관들에서는 정보가 기록되지만 거의 검열해 보지 않아서 어떤 심각한 보안위반행위가 있었는지 잘 모르고 있다. 보안이 단순한 기술이상의것이라는것을 고려하면 보안관리공정은 그 보안에 쓰이는 기술과 그 책임을 맡은 사람들의 자격과 꼭같이 중요하다. 기술적으로 준비된 보안관리자들은 자기들이 관리하는 기술을 알아야 할뿐아니라 보안에서 기술의 역할과 같은 기술의 보안상 중요성도 반드시 알아야 한다.

기록파일관리와 그것을 실행할 해당기술인원문제는 기업의 보안방책에서 제기되는 보안관리계획의 한 부분으로 되여야 할것이다.

자료교환과 보관

보안정보교환을 위한 업계표준이 없으므로 보안정보관리에서는 큰 문제가 제기되고 있다. XML표준이 이 공간을 메꾸어 줄것으로 보고 있지만 업계에서는 아직 널리 보급되지 못하고 있다. 따라서 사용자들은 판매업체가 정보교환표준을 채택할것을 바라고 있지만 말고 판매업체들이 제공한 각이한 형식으로 각이한 원천의 보안정보들을 관리할 생각을 하여야 한다.

XML과 같은 보안정보교환표준은 한걸음에 지나지 않는다. 장기적관점에서 볼 때 난관은 동일한 보안공간에서 각이한 제품에서 나오는 보안정보를 공통적으로 어떻게 분류하겠는가 하는 문제이다. 실례로 IDS들은 자료분류를 꼭같이 하기때문에 어느 한 IDS가 생성한 보안사건이 다른 판매업체에서 구입한 IDS가 생성하는 류사한 보안사건과 동일한 방식으로 처리된다.

아직 자료교환을 위한 업계표준이 없지만 모든 제품들은 보안관련정보들을 하나의 자료기지에 보관할수 있는 능력은 있다. 개방형자료기지접속성(ODBC)을 준수하면 각이한 프로그람들과 자료기지들사이의 자료교환이 가능해 진다.

보관 즉 기억시키는데서 나서는 문제는 수집자료량과 기억방식의 결정이다. 표준적으로 자료기지를 설계하여 수집정보를 기억 혹은 보관시켜야 할것이다. 그 자료기지안은 보안사건들의 분류성격과 보관성격을 결정해야 할것이다.

보관요구사항들을 설계할 때 보안관리자들이 고려해야 할것은 예비본만들기와 예비본풀어보기특성들과 같은 알려 진 문제들이다. 기타 문제는 높은 리용성과 원격접근성을 제공하는것이다.

호상관계와 분석

기업전반의 보안적안목을 가지기 위해서는 보안정보가 회사전반에 걸쳐 종합되여야 한다. 이것은 기업망의 각이한 장치들(침입탐지체계, 방화벽, 체계호스트, 응용프로그람, 경로기, 교환기 등)에서 오는 정보들을 포괄한다. 이상의 정보들은 취약성자료와 함께 기관의 보안태세를 확인할수 있게 한다.

기록철자료분석

종국적으로 보면 보안정보분석은 해당 기술적위험을 더 잘 료해하자는데 그 목적이 있다. 또한 영업위험관리에도 유용한 정보로 될수 있을것이다.

정보종합원칙은 개별적부분들에서 오는 정보의 합이 부분들이 모여 진 전체에서 오는 정보보다 못하다는 사실에 기초하고 있다. 기업에서 생성된 있을수 있는 보안관계사건들의 수가 주어 지면 그와 관련된 보안전문정보나 사건을 의미 있게 련관시키는것이

곧 난관으로 제기된다.

IDS에 의하여 탐지된 보안사건은 기업의 DMZ에 있는 방화벽이나 Web봉사기가 기록한 류사한 사건과 관계되는것일수 있다. 사실 이러한 사건은 DMZ뒤에 있는 후위처리콤퓨터들의 특정한 활동과 관계되는것일수도 있다.

사건들의 호상관계는 보안관계사건의 성격에 대하여 통찰력을 가지게 한다. 그리하여 기관망에 주는 일이 일어 났다고 하면 그 사건이 어떻게 되여 일어 났는가 하는데 대한 각이한 흐름의 씨나리오를 써낼수 있다.

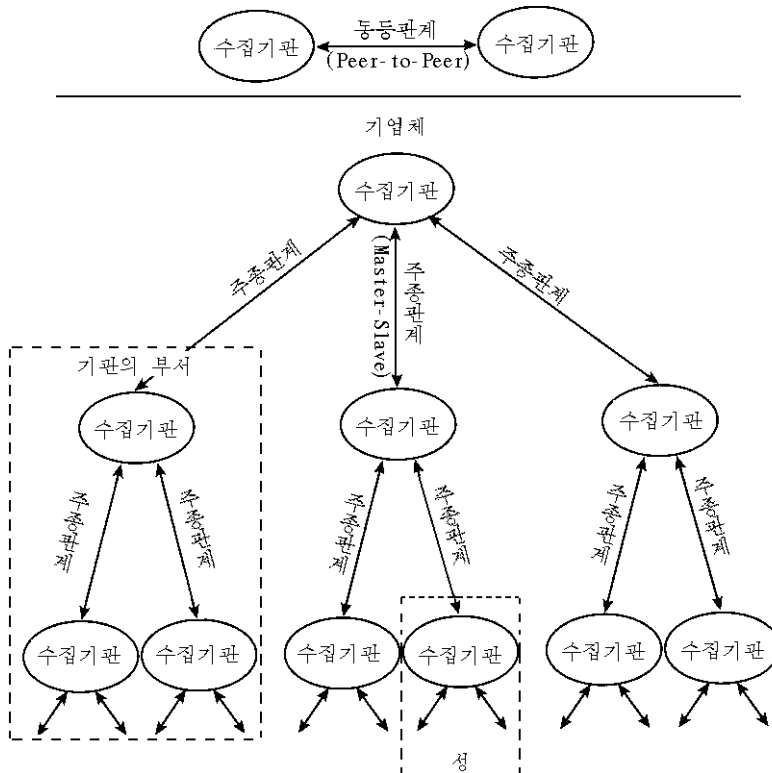



그림 25－1. 정보수집과 호상관계

비무장지대(DMZ)에 설치된 IDS에 의해 탐지된 사건의 례를 들어 보자. 방화벽이 이것을 탐지하지 못하였다고 보자. 그것은 방화벽설정을 제대로 잘하지 못한 탓일수 있다. 방화벽이 만일 그 사건을 탐지하고 차단하였다면 좋을것이다. 그러나 그렇게 하지 못하였다면 조사를 하여야 한다. DMZ에서 Web봉사기가 잡아 내였다면 그때에는 우려해야할 근거가 있다. 호상관계는 또한 공격 받는 장치의 중요성에 기초하여 해당한 반응을 결부시켜 주기도 한다.

방화벽에서 관찰되는 보안사건들을 방화벽에서 관찰되는 사건들 그리고(필요하면) DMZ와 지어 DMZ뒤에 있는 후위응용프로그람들에서 일어 나는 사건들과 련결시켜 보는것이 그럴듯하다. 결과 얻어 진 종합적인 정황판단결과는 강력하여 기관의 보안관계사건

들을 보다 총체적으로 보여 준다.

사건호상관계를 잘 그리려면 기업전반의 전략이 내용 있게 되여야 한다. 그림 25－1은 정보의 수집과 호상관계에 대한 하나의 구성방식을 보여 준다. 이 실례에서는 동등관계로 설정된 수집자들과 주종관계로 설정된 수집자들을 보여 준다. 동등관계의 수집자들은 의견교환에서 류사한 통제를 할수 있다. 주종관계는 그 문제안의 통제권을 보유하고 있다.

일이 잘 되자면 그리고 기관의 보안태세의 총체를 보여 주자면 수집자들은 여러가지 다양한 원천 즉 사건기록파일, 체계기록파일, 침입탐지체계, 방화벽, 경로기, 교환기들에서 나오는 모든 정보들을 처리할수 있는 능력을 가져야 한다. 특별수집자들을 망장치(례하면 방화벽)들에 배치하면 방화벽보안설정을 한눈에 볼수 있을것이다.

우의 실례는 수집자들이 기업전반에 배치되였으나 기업구성방식에 따라 배치된 가능한 하나의 씨나리오를 보여줄따름이다. 이렇게 되면 기업의 각 단위들이 자기단위의 정보를 수집하여 자기 선을 따라 해당 플래그신호가 있는 정보만 종합적형태로 올려 보내여 기업보안태세에 대한 종합적그림을 그리는데 도움을 줄수 있다.

정보보고체계를 달리 조작할수 있는 다른 모형도 있을수 있다. 실례로 수집자배치방식을 동등위치관계, 주종관계로 할수도 있고 량자를 결합시키는 방식으로 할수도 있다. 각 기관들은 어느 모형이 자기들에게 가장 적합한가에 대하여 결심채택을 잘 하여야 한다.

취약성자료

기록자료분석과 호상련계설정이 물론 기관의 《적극적보안》의 한 구성요소로서 중요하기는 하지만 그것만 가지고서는 기업보안태세를 충분히 담보할수 없다.

표준적으로 볼 때 망평가자료에서 취약성자료들을 가져 다 더 분석해 보아야 한다.

취약성자료라고 하면 그것은 대체로 열려 진 포구의 개수, 가동중인 봉사형태들, 해당 봉사가 막기 힘든 정보로출형태, 이 정보로출의 잠재적심각성과 같은것들을 발견하는데 목적을 둔 스캔을 말한다.

취약성자료들을 어떻게 관리해야 하는가에 대한 지침서는 현재 얼마 없다. 그러나 자료채취를 하면 다음의 측면들을 포함한 내용을 알수 있게 된다.

- 해당 망토막에서의 취약성개수에 기초한 위험상태표(례 : 매 망당 위험상태, 매 부서당 위험상태 등)
- 고위험도 및 저위험도취약성비률에 대한 측정값
- 각이한 시점의 스캔에 기초한 취약성자료의 경향지표, 이러한 경향들을 보간하거나 외삽하면 현보안상태에서 개선될 점들을 명백히 알수도 있고 또 개선되였는가 하는것도 알수 있다.

특별위험상태표들은 근원분석에 유익하다. 일부 취약성위험상태표들을 보면 보안계획작성, 설계, 실행과정과 같은 수많은 요인들과 관련된 특유한 약점들과 함께 보안공정의 강도 같은것을 잘 알수 있다.

보안실행자들에게 있어서 난관은 보안관리를 개선할수 있도록 취약성자료를 제공하는 최선의 방도를 결정하는것이다. 구체적으로 보면 호상련계설정으로부터 얻은 교훈, 취약성자료에서의 경향성, 성능측정값과 함께 근원분석 등을 념두에 둘수 있다. 또한 이 내용들도 보안관리에 유용하지만 최종목적은 결국 기술적취약성정보를 기업위험과 련관시켜 보는것이다. 총체적자료는 충분하지 못해도 일정한 취약성자료를 장악하면 있을수 있는 기업위험이 어떤 형태로 나타나겠는가 하는것을 알수 있다. 돈 파커와 같은 일부 사람들은 이런 방법이 적합하지 않다고 본다. 파커는 있을수 있는 보안사고를 피하는데 드는 비용은 절대로 량적으로 계산할수 없다는 사실에 기초하여 응당한 관심을 돌릴것을 주장한다.

요약과 결론

기업안에는 각이한 보안정보원천이 있어서 보안정보를 여러가지 망기능을 수행하는 장치들로부터 받아 본다. 방화벽이나 침입탐지체계와 같은 기술들이 보안강화에서 관건적역할을 한다면 경로기, 교환기나 체계기록파일들에서 나오는 정보들은 기관의 보안상태를 단번에 보여 준다.

보안관리자들에게는 보안관리공정에 통보하고 그 공정을 개선할수 있는 방향에서 정보를 수집, 보관, 분석해야 하는 어려운 과업이 나서고 있다. 보안은 기술에 상당히 의존하지만 이 문제는 여전히 보안을 담당한 사람들과 보안을 둘러 싼 공정과 관련된 문제라는것을 잊지 말아야 한다.

정보수집전략에는 전략적위치들에 려과체계를 응용하는것도 있는바 이때 통과되여야 할 정보만 통과시키는 려과장치가 완벽해야 한다. 지능형요소들을 리용하면 정보수집과 종합을 사용성 높게 진행함으로써 중앙에서 집계된 정보량을 최소화할수 있게 될것이다. 보안관리앞에 나선 또 하나의 어려운 과업은 기업보안의 여러 측면들에 대한 측정기준을 세우는것이다. 여기에는 특정한 위험성이 있는 망장치들의 백분률 같은 계측자료들이 속한다. 또한 이 계측자료들을 리용하여 근원분석함으로써 콤퓨터사용환경에서 제기되는 문제들을 발견하고 해명할수도 있다. 그 이외의 문제는 기술적측정값과 기업위험측정값과의 련관관계를 맺어 주는 능력이다.

또 있다. 일정한 기간안에 기술적위험수를 장악하면 경향성을 찾아 낼수 있다. 이 경향성은 일정한 기간안에 기관의 보안태세를 확립하는데 개선이 있었는가를 보여 준다.

망기술의 기능들을 리해하는것외에도 여러가지 기타 난관들이 보안 및 위험관리자들에게 제기된다. 보안관리가 매우 복잡한 과정이라는 현실을 제껵 파악하는것은 일단계에 지나지 않는다. 다음단계는 정보관리공정들과 방도들을 명백히 규정하는것이다. 보안공정에 통지하여 보안태세향상에 기여하도록 하는 방향에서 정보를 리용한다면 그것은 하나의 큰 공적으로 될것이다. 마지막으로 기업위험관리에 실지 쓸수 있는 계측지표들과 경향성을 명확히 규정하는것은 앞으로 하나의 중요한 과제로 나설것이다.

참 고 문 헌

1. Zwicky, E.D., Cooper, S., and Chapman, D.B., *Building Internet Firewalls,* 2nd edition, O'Reilly, 2000.
2. http://csrc.nist.gov/publications/nistpubs/800-7/node155.html.
3. Wack, J. and Carnhan, L., Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls. NIST Special Publication 800-10. U.S. Department of Commerce. National Institute of Standards and Technology, February 1995, http://csrc.nist.gov/publications/nistpubs/800-10/main.html.
4. Ballew, S.M., *Managing IP Networks with Cisco Routers,* 1st edition, O'Reilly, 1997.
5. Goncalves, M., *Firewalls Complete,* McGraw-Hill, 1998.
6. Syslog the UNIX System Logger, http://www.scrambler.net/syslog.htm.
7. http://njlug.rutgers.edu/projects/syslog/.
8. Explanation and FAQ for RME Syslog Analyzer, http://www.cisco.com/warp/public/477/RME/rme_syslog.html.
9. Marshall, V.H., Intrusion Detection in Computers. Summary of the Trusted Information Systems (TIS) Report on Intrusion Detection Systems, January 1991.
10. Carson, M. and Zink, M., NIST Switch: A Platform for Research on Quality of Service Routing, 1998, http://www.antd.nist.gov/itg/nistswitch/qos.spie.ps.
11. Parker, D., Risk Reduction Out, Enablement and Due Care In, in *CSI Computer Security Journal,* Vol. XVI, #4, Fall 2000.
12. Nyanchama, M. and Sop, P., Enterprise Security Management: Managing Complexity, in *Information Systems Security,* January/February 2001.
13. Base, R. and Mell, P., NIST Special Publication on Intrusion Detection Systems.
14. Security Portal; The Joys of the Incident Handling Response Process.
15. Ranum, M., Intrusion Detection Ideals, Expectations and Realities.
16. NIST Special Publication, 800-12, Introduction to Computer Security, *The NIST Handbook.*

제２６장. 구성관리

몰리 크렌케
데이비드 크렌케

구성관리(CM)는 보안실행에서의 일관성, 완전성, 엄밀성을 보장한다. 구성관리는 또한 하나의 공정이며 방도로서 기관의 현보안태세 즉 사용되는 기술, 수행되는 공정들과 실천, 기업보안상태의 변화에 주는 영향을 분석하는 도구로 복무한다. 새로운 기술의 도입이 일정에 오르면 여러가지 관점에서 분석해봄으로써 그 효과를 결정할수 있다.

- 구입, 설치, 유지 및 감시 비용
- 현존기술 및 구성요소들과의 긍정적 및 부정적호상관계
- 성능
- 보호수준
- 사용상편리
- 그 기능을 실현하기 위하여 수정해야 할 관리방식
- 그 새로운 기술의 정확한 리용을 위한 사용자 및 제공자양성과 관련되는 인적자원

구성관리기능들은 기관의 현보안상태를 조종하여 기관의 목적을 달성하는데서 미래의 길을 밝혀 주는 근본문제로 된다. 그러나 과정적인 견지에서만 구성관리를 대하게 되면 기관의 정보보안상태를 개선하며 사업성과를 지원하는 중요한 공정들을 보지 못하는 결과를 초래할수 있다.

체계보안능력성숙모형(SSE–CMM)은 주요요소들과 방책들, 절차적인 실례들을 제시하는데 리용된 장기적안목이 있는 기성참고서들과 함께 CM의 서술에서 기본틀거리를 이루게 될것이다.

SSE–CMM에 대한 개괄

SSE–CMM은 보안처리를 정확히 함으로써 하드웨어, 쏘프트웨어자료를 비롯한 기관의 정보자원들을 보호할수 있는 기관내 보안공학적과정의 기본특징들을 서술하고 있다. SSE–CMM모형은 다음의 문제들을 다룬다.

- 개념정의, 요구분석, 설계, 개발, 통합, 설치, 운영, 유지보수, 페기과정을 포괄한 전체 체계의 생명주기
- 경영진의 사업, 부서별 사업, 공학적활동들을 비롯한 기관전체와 개발자, 통합자들을 비롯한 보안봉사를 진행하는 전체 부서성원들

표 26-1 정보보안발기안들

명칭	목적	방법	범위
SSE–CMM	보안공학능력을 정의, 개선, 평가하는것	지속적인 보안공학의 성숙모형과 평가방법	보안공학기관들
SE–CMM	체계 및 제품공학공정의 향상	체계공학실천과 평가방법의 지속적인 성숙모형	체계공학기관들
쏘프트웨어를 위한 SEI–CMM	쏘프트웨어개발관리의 향상	쏘프트웨어공학 및 관리 실천의 단계적성숙모형	쏘프트웨어공학기관들
신뢰성 있는 CMM	높은 무결성쏘프트웨어개발공정과 그 환경의 개선	쏘프트웨어공학운용 보안의 단계적성숙 모형	높은 무결성 쏘프트웨어기관들
CMM1	현존공정개선모형들을 단일구조형식으로 통합하는것	공정개선구성요소들을 분류, 통합, 배치하여 필요한 모형을 만든다	공학기관들
Sys, Eng, CM (EIA구31)	체계공학능력의 정의, 향상, 접근	지속적인 공학적성숙 모형과 평가방법	체계공학기관들
공동기준	재사용성보호자료들을 기술강의에 리용함으로써 보안을 향상시키는것	보안의 기술적 및 담보적 요구사항들과 함께 평가공정수립	정보기술
CISSP	보안전문가라는 학문분야를 사회적으로 인정하게 하는것	보안지식총체와 보안 전문가 자격시험	보안실천가들
담보틀거리	넓은 범위의 증거를 제공함으로써 보안 담보를 개선하는것	체계적인 방법으로 담보론리를 전개하여 효과적으로 증명하는것	보안공학기관들
ISO 9001	기관적인 품질관리를 개선하는것	품질관리공정에 대한 구체적인 요구사항	봉사기관들
ISO 15504	쏘프트웨어의 공정 및 평가의 개선	쏘프트웨어공정개선 모형과 평가방법	쏘프트웨어공학 기관들
ISO 13335	정보기술보안관리의 개선	해당수준의 정보 및 봉사의 보안을 달성하고 유지하는데 필요한 지도와 일정	보안공학기관들

- 체계들, 쏘프트웨어, 하드웨어, 인적요인들과 같은 기타 분야와의 동시적인 호상관계; 체계관리, 체계운영, 체계유지 및 보수
- 구입, 체계관리, 보증, 인가, 평가를 비롯한 기타 기능들과의 호상작용
- 상업기관, 정부기관, 학술기관 등 각종 보안관련기관들

SSE-CMM과 기타 발기안들과의 관계

표 26－1에서는 SSE–CMM이 정보체계보안과 보안공학의 구조, 일관성, 담보성과 전문가수준을 다루는 다른 발기안들과 어떤 관계가 있는가를 보여 준다.

CMM틀거리

> CMM은 림시적이며 덜 조직화되고 덜 효과적인 상태로부터 고도로 구조화되고 효과적인 상태로 보안공학기관을 만들어 내기 위한 하나의 틀거리이다. 이러한 모형을 사용하면 각 기관들은 보안실현을 통계학적공정의 조종하에 진행함으로써 그 처리능력을 높이는 하나의 수단으로 된다. SSE–CMM은 보안공학에 통계적공정조종의 개념을 도입하면 예상된 범위의 원가, 시간표, 질범위내에서 안전체계와 신뢰제품의 개발이 촉진될것이라는것을 예견하여 개발되였다.
>
> –SSE–CMM 2.0판, 1999년 4월 1일

> 하나의 공정이란 해당 목적을 달성하기 위하여 수행되는 활동들의 모임을 말한다. 정확히 정의된 공정에는 활동들, 비활동의 입구 및 출구결과물들, 그 활동수행을 조종하는 장치들이 속한다. 정의된 공정은 기관이 공식적으로 해석하며 그 기관의 보안전문가들이 사용할수 있게 하며 어떤 행동을 취하여야 하는가 하는것도 밝혀 주어야 한다. 수행된 공정은 실지 보안전문가가 실행한 행동이다. 공정성숙은 해당 공정의 정의, 관리, 계측, 조종, 효과의 정도를 보여 준다. 공정성숙은 잠재적인 능력개선을 알려 주며 기관의 공정과 그것이 기관전반에 구현된 일관성정도들의 풍부성을 다 같이 보여 준다.
>
> –SSE–CMM 2.0판, 1999년 4월1일 –

보안공학성숙과 관련된 능력수준

SSE-CMM성숙모형과 관련하여서는 능력의 개성을 보여 주는 5가지 능력수준이 있다(그림 26－1 참조). 성숙정도에 따라 능력수준의 순서를 정하였으며 매 수준에는 일반화된 실천내용을 보여 주었다. 따라서 보다 높은 수준의 공정능력을 보여 주는 일반화된 실천내용들은 능력항목들의 제일우에 놓인다.

> SSE–CMM은 일반화된 실천내용의 실현에 대한 구체적인 요구사항을 제시하지 않는다. 각 기관들은 공정의 계획, 추적, 정의, 조종, 개선을 자기의 실정에 맞게 자유롭게 진행할수 있다. 그러나 웃준위의 일반실천이 아래준위의 일반실천에 의존하게 되기때문에 아래준위의 일반실천을 진행한 다음에 웃준위일반실천을 수행하는것이 좋다.
>
> –SSE–CMM, 제2.0판 1999년 4월 1일–

기초실천이 진행됨	· 실행결의 좋다. · 실행을 계획화한다. · 실행에서 규률 있다. · 실행을 추적한다. · 실행을 확인한다.	· 표준공정을 정의한다. · 표준공정을 자기 실정에 맞게 수행한다. · 자료를 리용한다. · 정의된 공정을 수행한다.	· 측정가능한 품질목표를 설정한다. · 목적달성을 위한 공정능력을 결정한다. · 객관적으로 실행을 관리한다.	· 량적공정효과성 목표를 설정한다. · 공정효과성을 높인다.

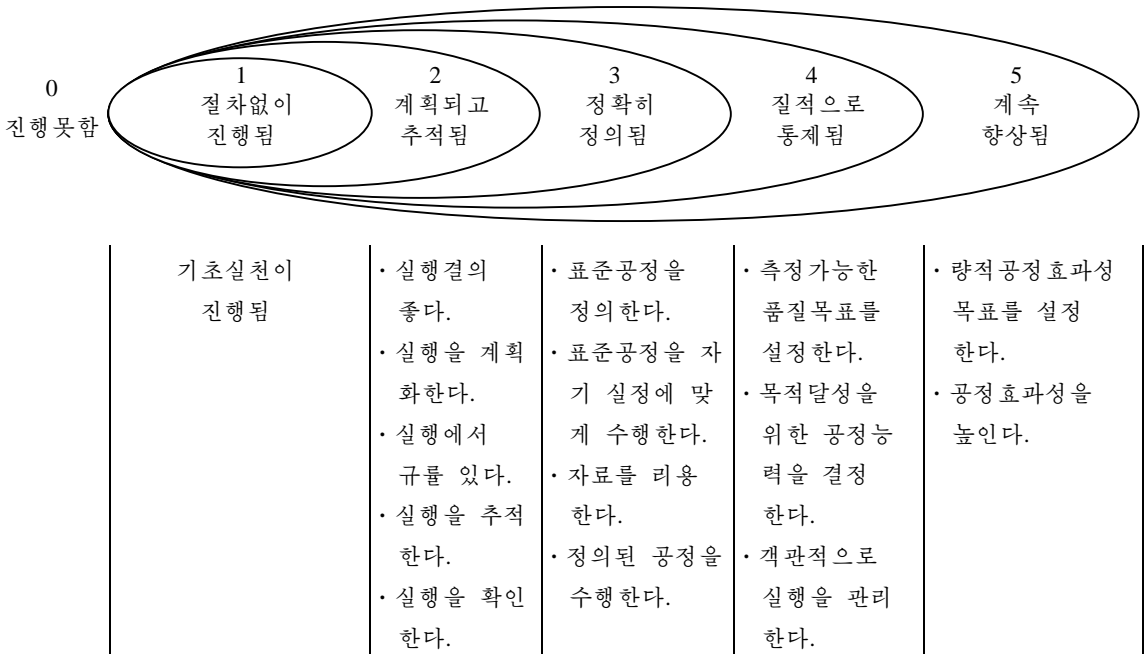



그림 26－1. 보안공학기관의 능력수준

CMM의 제도화

제도화는 하부시설과 기업문화의 수립으로서 방법, 실천, 절차들을 그 초기정의자들이 사라진 후에도 구축하여 준다. SSE–CMM의 공정능력측면은 정량적관리와 지속적개선에로의 실천과 방향을 밝혀줌으로써 제도화에 도움을 준다. CM공정과 그 관련 기초실천들이 성숙되고 지속적으로 개선되면 다음의 특성들을 가지는 활동들을 진행할수 있다.

- **지속성** 이전에 체득한 지식이 앞으로도 리용된다.
- **반복성** 개발계획들이 계속 성공을 반복하게 하는 방도
- **효률성** 개발자들과 평가자들이 보다 효률적으로 일할수 있는 방도
- **담보성** 보안요구가 해결된다는 확신

보안공학모형의 목표

SSE–CMM은 가장 널리 알려 진 보안공학실천들의 집합체이며 새로 태여나는 분야이다. 그러나 여기에도 일련의 총체적목표가 있다. 이 목표들은 정보자원의 보호를 위하여 투쟁하는 기타 기관들(표 26－1 참조)의 지원을 받고 있는것들도 많다.

- 기업의 보안위험에 대한 리해를 도모하는것
- 밝혀 진 위험요소들에 따라 균형적인 보안요구안을 수립하는것
- 보안요구사항을 보안지도에 구현하여 다른 분야의 사업에 통합시키며 체계설정과 체계운영지도서에 반영하는것
- 보안의 제도적장치의 정확성과 효과성에 대한 신뢰를 구축하는것
- 체계나 그 운영에 남아 있는 잔여적인 보안상 취약점들이 운영상 영향이 허용될수 있는것인가에 대하여 결심채택하는것
- 모든 보안공학관련분야와 전문부문들의 노력을 합치여 하나의 체계의 신뢰성을 일치하게 리해하도록 하는것

보 안 공 학

정보기술보안이 현시기 보안 및 기업환경에서 추동력으로 되는 분야이기는 하지만 보다 전통적인 보안분야도 결코 도외시하지 말아야 한다. 이러한 기타 보안분야들은 다음과 같다.

- 운영보안
- 정보보안
- 망보안
- 물리적보안
- 인적보안
- 행정적보안
- 통신보안
- 방사성보안
- 콤퓨터보안

보안공학적공정에 대한 개괄

보안공학적공정은 위험관리, 공학, 담보의 세가지 기본분야를 포괄한다. 위험관리공정에서는 개발된 제품이나 체계에 들어 있는 위험요소들을 발견하고 그 순위를 매겨 놓는 공정이다. 보안공학공정은 다른 공학분야들과 협동하여 그 위험요소들이 제기하는 문제에 대한 해결방도들을 찾아 내고 실현하는 공정이다. 담보공정은 보안해결책에 대한 신뢰를 구축하고 고객들이나 경영진에 그 신뢰를 전달하는 공정이다. 이러한 작은 공정들은 서로 협동하여 보안공학공정결과로 설정된 목표를 달성하도록 한다.

위험관리. 위험관리는 위험요소들, 취약점들, 그 영향들을 다룬다. SSE–CMM의 한 공정인 위험관리는 위험을 발견하고 그 량을 측정하여 기관에 접수될수 있는 수준의 허

용위험을 확정하는 공정이다. 위험관리공정을 지원하는 보안실천분야들은 보안위협분석, 영향분석, 취약성분석분야들이다.

공학. 보안기사들은 고객들과 협동하여 밝혀 낸 위험요소들, 해당법률, 기관의 방책들과 현존 정보설정값들에 기초하여 보안요구사항들을 확정한다. 보안공학은 개념, 설계, 실행, 시험, 전개, 운영, 유지보수, 페기를 포괄하는 공정이다. 이 공정은 체계공학팀의 기타 부분과 긴밀히 협조하고 의견을 나누어 해당 목적을 달성하기 위한 활동들을 조절함으로써 보안이 그 공정의 전일적인 하나의 요소로 되도록 할것을 요구한다. 일단 보안필요사항이 확정되면 보안기사들은 구체적인 요구사항들을 확정해야 한다.

공학적공정을 지원하는 보안실천분야는 보안의 필요성들을 지적하며 보안상 입력항목을 제시하며 보안통제를 실시하며 보안태세를 감시하는것들이다. 생명주기의 후반기에는 보안기사들로 하여금 제품들과 체계들이 예견되는 위험성들과의 관계에 부합되게 정확히 결정되였는가를 확인하게 함으로써 새로운 위험요소들이 체계가 불안전한 운영을 하지 않게끔 하는것이 필요하다.

담보. 담보는 보안상요구가 만족되였다는 신뢰성의 정도를 말한다. 통제가 실현되였고 또 앞으로도 예견한대로 작용할것이며 예견된 위험을 줄일것이라는 담보는 흔히 론증의 형식으로 통보되며 보안공학적활동의 정상과정에 만들어 진 문건으로 확인되게 된다.

보안공학의 기초적인 공정분야들

SSE–CMM은 약 60가지의 보안기준실천사항들을 담고 있으며 보안공학의 모든 주요분야들을 포괄하는 11개의 공정분야로 되여 있으며 현재 보안공학계의 가장 좋은 실천내용들을 반영하고 있다.

기준실천들은 기업의 생명주기전반에 해당하며 기타기준실천들과 겹치지 않으며 보안부문에서 하나의 최선의 실천으로 되며(최첨단기법으로는 되지 못함) 다중적인 기업환경에 다중적인 방법을 사용할수 있게 하며 특수한 방법이나 도구를 구체적으로 지정하지 않는다. 11개의 SSE–CMM공정부문들을 아래에 제시하였는데 하나의 실천을 생명주기의 한 단계로 보지 말아야 한다.

- 보안통제를 실시한다.
- 영향을 분석한다.
- 보안위험을 분석한다.
- 위험요소들을 분석한다.
- 취약성을 분석한다.
- 담보의 근거를 마련한다.
- 보안을 조정한다.
- 보안상태를 감시한다.
- 보안입력사항을 제시한다.

- 보안요구사항을 구체화한다.
- 보안을 확인하고 비준한다.

보안공학의 개발계획과 기관적인 실천

개발계획과 기관적인 실천과 관련되는 11가지의 공정분야들도 있다.

- 질을 보장한다.
- 구성을 관리한다.
- 개발계획의 위험을 관리한다.
- 기술적노력을 감시하고 조종한다.
- 기술적노력을 계획화한다.
- 기관의 체계공학공정을 정의한다.
- 기관의 체계공학공정을 개선한다.
- 계렬제품(product line) 형성을 관리한다.
- 체계의 공학적지원환경을 관리한다.
- 계속 숙련하고 지식을 습득한다.
- 상품제공자들과 조정한다.

기준실천항목들과 개발계획 및 기관적인 실천항목들을 제시한것은 독자에게 이 장이 설정관리의 리용과 실천에 초점을 두고 있다는 관점을 주자는데 목적이 있다.

구 성 관 리

여기에서는 SSE–CMM PA 13항목 즉 《구성관리》와 관련한 기준실천사항들을 보여 주고 기관의 정보자원보안의 수립, 실행, 개선에서 나서는 방책, 절차 및 자원들을 다룬다.

구성관리에 대한 해설

구성관리(CM)의 목적은 밝혀 진 구성단위들에 대한 자료와 그 단위들의 상태를 유지하며 체계와 구성단위들에서 나타나는 변화들을 분석조종하는것이다. 체계구성을 관리한다는것은 개발자들과 고객들에게 정확한 현 구성자료들과 상태를 제공한다는것을 말한다. 목표는 기성사업결과구성에 대한 통제 및 조종을 실현하는것이다.

구성관리의 기준실천사항

다음의것들이 정확한 보안공학적CM의 핵심요소라고 볼수 있는 기준실천사항들이다.

- CM의 방법론을 수립하라.
- 구성단위들을 식별하라.
- 사업결과들의 기준선들을 보존하라.
- 설정된 구성단위에 대한 변화를 통제하라.
- 구성상태를 통보하라.

매개의 기준실천사항들을 아래에서 구체적으로 보자. 서술방식은 SSE–CMM에 대한 해설, 모범으로 되는 사업결과, 그에 대한 설명으로 순서가 되여 있다. 그 다음에는 기준실천사항을 실현하는데 리용될수 있는 기타 참고서들과 자원들을 제시한다.

구성관리의 방법론을 수립하라

다른 보안참고서들과의 호상관계

CM공정을 지원할수 있는 CM도구를 선택하는것은 기업공정들과 구성될 해당 자원들에 달려 있다(표 26−2 참조).

표 26−2 BP.13. 01–CM방법론을 수립한다

해설

CM의 구조와 원가에 영향을 줄수 있는 세가지 기본선택안들은 다음과 같다.

- 구성단위선택의 구체화수준
- 구성단위들이 CM밑에 들어 가는 시기
- CM과정에 필요한 절차화수준

사업결과의 실례

- 구성단위들을 선정하는 기준지표
- 구성단위들을 CM밑에 맡기는 시간선
- 선택된 CM공정
- 선택된 CM공정해설서 설명

주의

구성단위에 대한 선택기준들은 대면부보수유지, 사용자의 독특한 요구사항,
새 설계 대 개조설계관계, 변화예견률 등을 고려해야 한다.

SSE–CMM, 제2.0판, 1999년 4월 1일, 213–214페지

《안전, 품질, 시간표, 원가, 환경에 영향을 줄수 있는 정보라면 그 어떤것이든 관리해야 한다. 공급사슬속에 있는 매 활동은 관리공정에 속해야 한다. …최상의 CM공정이란 변화에 가장 잘 적용할수 있으며 모든 해당정보가 명백하고 간결하며 가치를 가질수 있게 하는 공정을 말한다.》

CM공정은 그것이 실행될 조건과 환경과 결부되여야 한다. 관계된 활동들에서는 책임분담, 인원양성, 사업능률의 측정단위의 결정이 포함되여야 한다. 구성관리계획(CMP)을 세우면 CM과 국제표준화기구(ISO) 9000계렬의 품질체계기준을 호상 련결시킬수 있다. 이 계획을 세우면 또한 자동도구들을 비롯한 소요자원과 설비들에 대한 설명을 쉽게 할수 있다.

자동도구들

구성관리연구소. 구성관리연구소(ICM)에서 승인을 받은 도구들은 여러가지이다. 그 도구들은 ICM이 정의한(CMII로 표시됨) 하나의 (새로운) 구성방법론을 지원할수 있는것으로 하여 승인을 받았다. 그 도구들은 표 26－3에 서술되였다.

표 26－3 ICM의 CMII이 승인한 자동도구들

체계부류	체계이름	출하 및 판본	제공자이름/싸이트	승인날자
PDM	Metaphase	3.2	SDRD/Methphase www. SDRD.com	2000년 5월 12일
PDM	Axalant–CM	1.4	Usb/Eiger+Partner www.usbmuc.com www.ep–ag.com	2000년 12월 8일

ICM의 승인은 다음과 같은 내용을 의미한다.

- 도구가 CMII기능들의 핵심요소들의 달성을 지원한다.
- 도구가 그 부류의 도구들에 필요되는 모든 분야의 기능들에서 강력성의 잠재력을 가지고 있다.
- 개발자는 CMII와 관련된 그 도구의 장점과 약점을 리해하고 동의한다.
- 개발자는 이러한 약점들을 극복하기 위하여 개선사업을 진행하기로 계획한다.
- 이렇게 하려는 개발자의 의견에 ICM은 동의한다.

기타자동도구들. IBM 메인프레임환경에서 리용되는 또 하나의 자동쏘프트웨어관리도구는 ENDEVOR이다. 이 제품은 체계가동을 위한 모든 프로그람 원천코드, 대상코드, 실행코드(적재모듈들), 번역기능코드, 조종정보, 해당 문건들의 이관을 자동화할

수 있다. 여기에는 고준위프로그람작성언어로 씌여 진 원천프로그람, 작업통제 및 기타 통제언어, 자료사전, 조작체계, 자료기지구성부문들, 직결원격처리체계, 작업절차 등이 포함되여 있다.

상업적으로 구매할수 있는 두가지 직결CM도구들은 UNIX의 원천코드조종체계(SCCS)와 수정조종체계(RCS)이다.

도구의 역할을 하는 구성관리계획과 구성통제위원회

콤퓨터보안기초. 이 참고서에서는 어떤 한 체계의 생명주기전기간에 걸치는 CM을 위하여서는 수동추적체계도 리용될수 있다고 밝히고 있다. CM실행과 관련한 방책들은 다음과 같다.

- 매 구성항목에 대하여 고유식별자를 붙일것
- CMP를 세울것
- 구성항목에서 나타나는 변화(직결이든 오프라인이든)들을 전부 기록할것
- 구성통제위원회(CCB)를 설립할것

EIA-649. 구성식별은 고유한 제품의 식별, 정의, 확인의 기초이며 제품과 문건의 식별표식, 변화관리, 책임성관계의 기초이기도 하다. 이 공정에서는 사용자가 제품판본들을 구별하게 하며 기준선관리를 위한 문건의 출하를 통제한다.

정보체계보안공학편람. CM은 하나의 체계(쏘프트웨어, 하드웨어, 펌웨어, 문건, 지원/시험설비, 개발/유지보수도구)에서 일어 나는 모든 변화들을 조종통제하는 공정이다. CCB를 구성하며 그 체계에서 일어 난 일체 변화를 검토하고 승인하여야 한다. 정보체계의 생명주기전반에 걸쳐 CM을 진행하여야 할 리유들은 다음과 같다.

- 체계생명주기의 소여지점에서의 기준선을 유지하는것
- 시간에 따르는 체계들의 자연적발전(체계들은 정적으로 존재하지 않는다)
- 재해(자연재해와 인적재해)에 대처한 비상계획작성
- 모든 확인 및 보증증거들을 다 장악하는것
- 체계의 생명주기전반에 걸쳐 체계의 무한한 자원의 사용은 증가할것이다.
- 구성항목식별
- 구성조종 및 통제
- 구성회계
- 구성검사

NCSC-TG-006, 신뢰성체계의 구성관리에 대한 리해안내. CCB를 통하여 CM공정을 도모하는 CMP와 인적자원도 역시 《도구》로 간주되여야 한다. CM이 잘되자면 개발계획의 착수직후에 주도세밀한 계획안들을 작성하여야 한다. CMP에는 체계의 CM을 실행하자면 무엇을 해야 하는가 하는것이 간단명료하게 서술되여 있어야 한다. 이 CMP에는

CCM참가성원들의 역할도 명시되여야 한다. 체계와 관련된 모든 사람들의 책임분담이 CMP에 명백히 세워 지고 명문화되여야 CM과정에 인적요인의 역할을 정확히 추동할수 있다. CMP의 한 부분에는 또한 필요한 절차들이 명시되여야 하며 일상적인 CM절차들과 현존 《비상》절차들도 포함되여야 한다. CMP는 실천을 위한 산 문건이므로 여기에는 추가와 변화가 있을수 있으나 세심히 평가하고 승인한 다음 실행함으로써 정확한 담보를 마련해야 할것이다.

CM에 사용되는 그 어떤 도구도 CMP에 정확히 문건화되여야 한다. 이 도구들은 《엄격한 구성통제하에 보존》되여야 한다. 이 도구들에는 변화통제에 쓰이는 양식들, 구성항목명명관계, 쏘프트웨어라이브러리와 모든 자동화된 도구들을 포함한다. 보고에 리용되는 모든 문건표본들도 역시 CMP에 해설서를 첨부하여 포함시켜야 한다.

정보체계보안공학편람, 국가안전보장국, 중앙안전보장부. CM공정이 있어 해당한 승인도 없이 보안위험을 증대시킬수 있는 수정현상들을 미리 막도록 하는것은 체계가동후 체계의 생명주기, 증명/인가, 재증명/재인가 활동들에서 고려해야 할 하나의 문제이다.

구성단위들을 식별하라

표 26－4와 표 26－5를 보라.

표 26－4 **BP.13.02－구성단위들을 식별하라**

해설

구성단위란 기준선에 함께 놓이는 하나 혹은 그이상의 작업결과(혹은 작업제품)를 말한다. CM을 위한 작업결과의 선정은 선정된 CM전략에 밝혀 진 기준사항에 기초하여야 한다. 구성단위들은 개발자와 고객들에게 리득을 줄수 있는 수준에서 선정되여야 하지만 결코 개발자에게 불필요한 행정적부담으로는 되지 말아야 한다.

작업결과의 례

- 기준선에 놓이는 작업결과구성
- 식별된 구성단위들

설명

현지교체의 요구사항을 가진 체계의 구성단위들은 하나의 해당 구성단위를 현지교체단위준위에 두고 있어야 한다.

SSE–CMM, 제2.0판, 1999년 4월 1일, 215페지

다른 보안참고서들과의 관계

AR 25-3, 륙군정보체계생명주기관리. CM은 4가지분야 즉 구성식별, 구성조종, 구성상태계산, 구성검토에 기본을 둔다. CM은 구성항목들의 생명주기전반에 걸쳐 진행되여야 정보체계의 신뢰도를 통제 및 개선할수 있다.

영국국가표준(BS7799), 정보보안관리, 제1부, 정보보안관리체계의 실천조례. 변화조종의 결여는 《체계 혹은 보안 실패의 공통적인 원인》이라고 한다. 변화조종에 대한 공식적인 관리와 실천은 설비, 쏘프트웨어 혹은 절차들에 절실히 필요하다.

콤퓨터보안기초. CM항목들에도 문건들과 시험계획, 기타 보안관련체계도구들과 시설들이 포함될수 있다.

표 26-5　　　　구성단위들의 실례

다음의 구성단위실례들은 《BP.0.02-보안구성을 관리하라》에서 인용하였음

- 모든 쏘프트웨어갱신정보의 기록들: 사용허가, 계렬번호, 모든 쏘프트웨어와 그 갱신판의 령수증(날자, 책임진 사람, 변화에 대한 설명)을 기록한다.
- 배포와 관련한 모든 문제의 기록: 쏘프트웨어배포과정에 제기된 문제와 그 해결여부를 기술한다.
- 체계보안구성: 체계하드웨어, 쏘프트웨어와 통신의 현상태(그것들의 위치, 담당자, 관련정보 등을 포함함)를 기술한다.
- 체계보안구성변화: 변화를 가져 온 사람의 이름, 변화에 대한 해석, 변화의 리유, 변화날자와 시간 등 체계보안구성변화에 대하여 기술한다.
- 확증된 모든 쏘프트웨어갱신정보의 기록: 변화에 대한 해설, 변화시킨 사람이름, 변화날자 등 모든 쏘프트웨어갱신정보를 기록한다.
- 신뢰쏘프트웨어배포에 대한 주기적인 개괄: 최근에 진행한 신뢰성쏘프트웨어의 배포정형은 난점과 그 해결과정까지 서술한다.
- 요구사항에 대한 보안상변화: 보안상리유 혹은 보안에 주는 영향으로 하여 제기되는 체계요구사항에서의 변화를 추적함으로써 변화와 그 결과가 의도적인것으로 되게 한다.
- 설계문건에서의 보안상변화: 보안상 혹은 보안에 주는 영향으로 하여 제기되는 체계설계에서의 변화를 추적함으로써 변화와 그 결과가 의도적인것으로 되게 한다.
- 조종실현: 구성세부를 포함하여 체계내의 보안조종실현을 서술한다.
- 보안후열: 계획된 조종실현과의 관계에서 체계보안조종의 현상태를 서술한다.
- 통제수단의 폐기: 보안통제수단페기나 기능정지절차를 파도적인 계획까지 포함하여 설명한다.

SSE-CMM, 제2.0판, 1999년 4월 1일, 115～116페지

DOD-STD-2167A, 방위체계쏘프트웨어의 개발. 이 군부표준은 페기된지 오래되였지만 구성식별단위들은 많은 체계개발자들에게 익숙된 개념이다. 그 단위들은 콤퓨터쏘프트웨

어구성항목(CSCI)들과 그에 해당하는 콤퓨터쏘프트웨어의 구성요소(CSC)들과 콤퓨터쏘프트웨어의 단위들(CSU)이다. 문건은 기능적기준선, 할당기준선, 제품기준선들을 설정하였다. 인도가능한 매 항목들에는 하나의 판본명, 출하, 변화상태, 기타 식별세부가 있었다. 구성통제는 문건화된 기성계획에 따라 실행되였으며 구성상태통계실현을 통하여 중지되였다.

EIA–649 고유식별자가 있으므로 해당 단위에 관한 공정, 날자, 사건, 시험, 문건들의 호상관계를 명백히 알수 있다. 문건까지도 고유식별자를 붙여 정확한 제품구성과 련관을 맺도록 하여야 한다.

기준선이란 알려 진 구성에서의 그 어떤 시간점에서 제품에 대한 합의된 해설을 의미한다. 복잡한 제품들에 한해서는 중간기준선도 설정될수 있다. 기준선은 하나의 도구로서 변경에 대한 승인을 받기 위하여 당국과의 일치성을 맞추는데 필요하다. 기준선에는 요구사항, 설계안, 제품구성, 운영단계기준선, 페기단계기준선들이 있다.

《정보분류: 기업실현의 지침》, 정보보안관리편람 어떤 일을 누가 수행할것인가. 구체화한 작업요구서와 같은 쏘프트웨어변화사항들을 기록한 검열/력사정보들과 기업에 필요한 기타 해당 문건들을 보존하는것은 사활적인 쏘프트웨어통계수단이다.

사업결과들의 기준선들을 보존하라

표 26－6을 볼것.

표 26－6　　　BP13.03－사업결과물기준선들을 보존할것

해설

이 실천사업에서는 사업결과물구성에 대한 종합정보를 구축하고 보전하며 …자료를 수집하거나 기준선추가, 삭제, 수정에 대한 이룩된 절차와 함께 구성자료의 추적/감시, 검열 및 통계절차를 포함한 구성단위들을 묘사함으로써 체계생명주기의 임의의 지점에서 검열흔적을 원천문건들에 다시 제공한다.

사업결과물의 례

- 결심자료기지
- 기준선화된 구성
- 추적성회로망

설명

해당 문건들에 갱신과 변경을 쉽게 하기 위하여 구성자료들은 전자적인 형식으로 보존될수 있다.

다른 보안참고서들과의 관계

EIA-649. 구성의 기준선복구(혹은 해당문건없이 새로 만드는것)는 품이 많이 들며 자금이 많이 든다. 설계정보와 성능정보가 없는 경우 사찰을 통하여 구성을 확정해야 하는데 이것은 운영 및 유지보수결정에 영향을 준다. 거꾸로 일을 하면 그 공정에는 자금이 매우 많이 든다.

《정보분류: 기업실현의 지침》, 정보보안관리편람 이 장은 《갱신검사를 받았거나 집합서고나 생산서고에 적재되여 있는 쏘프트웨어판본》들을 비롯한 판본통제와 구성통제의 중요성을 강조하고 있다. 《이러한 통제에는 이러한 사업과 관련된 오유보고감시와 해당 교정행동을 취하는것이 포함된다.》

새 련합공동모형(NAPM). NAPM은 하나의 공동모형으로서 보안기능, 구성관리기능, 품질담보기능을 전반적인 자동정보체계(AIS)보안공학공정과 결합시켜 준다. NAPM은 기관의 AIS와 효률적인 보안프로그람의 실현에서 CM이 얼마나 중요한가를 깊이 깨닫게 한다.

> CM은 현존 AIS에 대한 변화는 식별과 통제가 가능한 환경에서 진행되며 이 변화들은 안전한 제품, 체계, 봉사의 무결성이나 리용성속성에 부정적영향을 주지 않는다는 담보를 가지고 관리를 제공한다. CM은 체계에 가해진 모든 추가, 삭제, 변경이 그 체계의 무결성, 리용성, 비밀성을 손상시키지 않는다는 보충적인 보안담보준위들도 제공한다. CM은 절차화와 편견없는 검증을 통하여 실현됨으로써 AIS와 혹은 모든 해당문건들이 식별, 변화통제, 상태통제, 검열이라는 4가지 구성요소를 중시하면서 정확히 갱신되도록 한다.

설정된 구성단위들에 대한 변화를 통제하라

표 26－7을 볼것.

다른 보안참고서들과의 관계

영국국가표준(BS7799), 정보보안관리, 제1부, 정보보안관리체계의 실천조례 변화의 잠재적인 영향, 제안된 변경의 승인절차준수, 비성공적인 변화의 중지 및 회복절차 등을 분석평가하는것은 운영적변경공정에서 중요한 의의를 가진다. 쏘프트웨어통제를 지원하며 운영적체계파손의 위험을 줄일수 있는 방책들과 절차들은 다음과 같다.

- IT승인을 받은 임명된 서고관리자에 의한 프로그람서고갱신
- 비실행형규정의 제외
- 새 국정에 대한 심도 있는 검사와 사용자접수

표 26－7 BP.13.04 설정된 구성단위들에 대한 변화를 통제하라

해설

기준선작업결과물의 구성에 대한 통제를 유지한다. 여기에는 매 구성단위의 구성에 대한 추적, 가능한 새로운 구성의 승인, 기준선갱신들이 속한다 .작업결과물에서 발견된 문제점들이나 작업결과물을 변경시키기 위한 요청을 분석하여 그 변경이 작업결과물, 프로그람시간표, 원가와 기타 작업결과물에 미칠수 있는 영향을 판정한다. 만일 그 분석에 기초하여 작업결과물에 대한 변경안이 승인되면 그 변화를 작업결과물과 기타 유관분야에 결합시키기 위한 시간표가 작성된다. 변경된 구성단위들은 후열과 승인을 거쳐 출하된다. 변경사항들은 출하되기전까지는 공식성을 띠지 않는다.

작업결과물의 실례

새로운 작업결과기준선들

설명

변경통제조치들은 변경사항의 부류에 맞게 조절되여야 한다. 실례로 다른 구성요소들에 영향을 주지 않는 구성요소의 변경에 대한 승인공정은 보다 간단할수 있다.

SSE–CMM, 제2.0판, 1999년 4월 1일, 217페지

- 프로그람원천서고갱신
- 모든 운영용 프로그람서고들에 대한 갱신검열기록의 보존
- 비상사고에 대처한 쏘프트웨어의 이전 판본들의 보유

영국국가표준(BS7799)정보보안관리 제2부 정보보안관리체계의 기술설명서. 공식적인 변경통제절차들은 체계의 생명주기전반과정에 걸쳐 실행되여야 하며 그 변화들은 엄격히 통제되여야 한다.

EIA–649

변화관리를 위한 초기기준선에는 수행활동(즉 제품개발자와 제품공급자의)이 만족시키기로 합의한 요구사항들을 규제하는 구성문건이 포함되여 있다. 변화관리를 위한 설계출하기준선에는 제품의 제작, 건설, 구축 및 코드화에 리용되는 세부설계문건들이 포함되여 있다. 변화관리를 위한 제품구성기준선에는 제품의 요구사항에 대한 제품구성을 규제하는 설계출하기준선으로부터 나온 세부설계문건들이 포함되여 있다. 제품구성은 성숙구성으로 간주된다.

현 요구사항들, 설계출하기준선이나 제품구성기준선에 대한 변화들은 어떤 문제가 발견되였거나 제품개선이나 향상이 제기되였거나 고객의 요구가 있다거나 시장이나 공공법률에 의하여 불가피하게 된 조건이 있는 경우에 생기게 된다.

> 변화들은 후열과 승인을 위한 해당 수준을 결정하는데 편리하게 주요변화와 부차적인 변화로 분류되여야 한다. 주요변화란 큰 영향을 가지는 기준선화된 구성문건들의 요구사항(요구사항, 설계출하기준선 혹은 제품구성기준선)들에 대한 변화를 말한다. 이 주요변화는 해당한 모든 기능그룹이나 생산품개발팀의 협조와 검토를 받아야 하며 해당 승인당국의 승인을 받아야 한다. …부차적인 변화는 구성문건(출하된 설계정보)에 공정들이나 부분적인 곳에 수정 혹은 변경시키는것이나 고객의 요구에는 …영향을 주지 않는 그러한 변화를 의미한다. 변화청구를 정확히 평가하자면 변화에 대한 청구내용이 문건에 명확히 반영되여야 한다. 부차적인 변화까지 정밀하게 기입하여 예견하지 않았던 우발사태나 예상치 않았던 제품사고가 나는 경우 검열흔적이 구축되게끔 하여야 한다. 정확하게 접근할수 있는 기록들을 가짐으로써 이러한 사태에 드는 연구비용을 절약하는것은 부지런히 질서있게 변화처리한것을 충분히 상쇄하고도 남음이 있을수 있다.

청구된 변화가 줄수 있는 기술적, 자원적, 시간표적 및 원가적인 영향도 반드시 먼저 고려해 본 다음에 승인을 받고 실행해야 한다. 그 변화의 영향을 받거나 그 변화실행에 책임이 있는 부문별 기관들도 이 변화공정에 참가하여야 한다. 이 부문별기관들은 변화의 성과적인 실행에 영향을 줄수 있는 중요한 정보(다른 기관들은 가지고 있지 못하는)를 가지고 있을수 있다. 변화에 대한 고려항목에는 일차적인 의뢰기관의 요구사항들(례하면 지원쏘프트웨어, 부속품 혹은 수리부속 등이 있는가, 운영보수지시사항에 수행된 내용은 없는가 등)은 물론 지원기관들의 시간상 및 자원상 요구사항들과 변화의 긴박성문제도 포함되여 있어야 한다. 검증실행범위는 변화된 단위들의 량과 실행된 변화의 형태에 따라 다를것이다. 변화에 대한 검증기록과 필요한 지원기능들의 실행기록들이 반드시 보존되여야 한다. 해당구성에 대한 변경내용들은 반드시 승인을 받아야 하며 문건화되여야 한다.

FIPS PUB102, 콤퓨터보안승인과 인가를 위한 지도서. 변화통제공정은 암시적형태의 재승인이며 재인가이다. 이 공정은 개발공정과 운영공정에서 다 필요하다. 기밀응용시 변화통제는 요구사항, 설계, 프로그람, 절차적문건들뿐아니라 하드웨어와 쏘프트웨어자체에도 리용되여야 한다.

이 공정은 우에서 렬거된 제품들에 대한 기준선설정을 거쳐 개발과정에 시작된다. 일단 기준선이 설정되면 모든 변화에는 공식적인 변경신청과 위임이 필요하다. 모든 변화는 이미 있은 승인근거문건에 미치는 그 영향관계가 검토된다.

이러한 변화통제를 주관하는 실체는 CCB이다. 개발과정에 CCB는 개발과제운영위원회나 그와 류사한 그룹의 보조실무그룹으로 된다. 개발이 완료되자마자 CCB의 책임은 대체로 운영 및 유지보수실에 이전된다. CCB에는 다음과 같은 사항들을 책임진 보안대표가 있어야 한다.

- 해당변화가 보안에 적중한가를 결정한다.
- 필요한 보안후열과 필요한 수준의 재승인, 재인가에 대하여 결정을 내린다.
- 재승인사업을 하지 않으면 안되게 하는 긴박한 요인을 결정한다.
- 특별한 보안후열이 필요 없는 부차적인 변화같은것에 대하여 기술적인 보안평정

자의 역할을 수행한다.

매우 기밀적인 분야에 한해서는 모든 변화에 대한 승인 및 검사제도를 세우는 것이 필요하다. 비록 사소한 변화라고 할지라도 검사결과와 같은 해당 승인증명은 물론 모든 변화요소를 전부 기록해 놓아야 한다. 이 기록은 재승인과정에 검토되게 된다.

> 그 어떤 체계나 그 환경변화, 재승인과 재인가의 보안상 특징들이 필요하게 되는 조건에서 … CM은 이 변화를 감시하는데 가장 적중한 분야이다.

정보체계보안공학편람

> 체계, 부분체계 혹은 구성요소에서의 변화나 갱신(례하면 새로운 조작체계출하판들의 통합, 자료관리 응용프로그람의 수정, 새로운 상업적쏘프트웨어파케트의 설치, 하드웨어갱신이나 교체, 새로운 보안제품의 설치, 《신뢰성》구성요소의 대면부특성의 변경 등) 은 … 그 보안적전제를 위반하는것으로 될수 있다. 가장 강력한 구성통제절차로서는 실지 동작환경에서 그 체계에 대한 물리적 및 기능적검열을 주기적으로 진행하는것이다. 그 절차는 문건들 또는 알려 지거나 제기된 변경에 전적으로 의거하는것이 아니다. 잘 알려 지지 않았거나 문건기록이 잘 되지 않은 변화도 때때로 제기될수 있다. 이 변화들은 체계의 하드웨어, 쏘프트웨어, 상주자료에 대한 직접적인 사찰을 통해서만 검출할수 있다.

NCSC-TG-006, 신뢰성체계의 구성관리에 대한 지침. CM은 체계의 생명주기전반에 걸쳐 그 체계에 대한 통제를 진행함으로써 운영되는 체계가 정확한 체계라는것을 담보하며 정확한 보안방책을 실현한다. 《보증통제목적》(Assurance Control Objective)은 구성관리에 다음과 같이 적용될수 있다.

> 기밀 혹은 극비정보를 처리보관하는 콤퓨터체계들은 그 하드웨어와 쏘프트웨어에 의거하여 그 정보를 보호한다. 이로부터 그 하드웨어와 쏘프트웨어자체가 비법적인 변경으로부터 보호되여야 그 보호장치들이 비정상가동이나 우회되지 않을수 있다는 결론이 나온다. 이렇게 되여야만 보안방책에 대한 하드웨어적 및 쏘프트웨어적인 실행이 정확하고 외곡없이 준수되고 있다는 신심이 생길수 있다.

구성상태를 통보하라

구성상태는 기관들의 사업의 성공에서 사활적이다(표 26−8 참조). 기관이 사용하는 정보는 정확하여야 한다. 《설계도가 잘못되였는데 집은 지어서 무슨 의의가 있는가》하는 격이 될수 있다. 모든 변화들을 신속하게 일관하게 문서화하고 통보해야 한다.

표 26-8　　　　　　　　BP. 13.05 구성상태를 통보하라

해설

상태변화가 있는 경우에는 언제든지 구성자료상태를 해당 그룹에 통지하라. 상태보고서에는 접수된 구성단위변화들이 언제 처리되는가에 대한 정보, 그 변화를 받은 해당 작업결과물에 대한 정보를 반영하였다. 개발자와 고객들과 기타 관계자들에게 구성자료와 구성상태에 대한 접근이 제공되여야 한다.

작업결과물의 례

상태보고서들

설명

구성상태통보활동에서 대표적인것으로서는 합법적사용자들에게 접근권을 제공하는것, 합법적사용자들의 기준선복사본들을 임의의 시간에 볼수 있게 하는것이다.

SSE–CMM, 제2.0판, 1999년 4월 1일 218페지

다른 보안참고서들과의 관계

EIA-649. 제품에 대한 구성관리정보는 생명주기와 해당 CM공정들(계획과 관리, 식별, 변화관리, 검증과 검열)전반에서 중요하다. 《구성상태통계(CSA)는 이러한 조직화 된 수많은 정보에 대한 관점들을 호상련결시키며 보관하며 보존하며 제공한다. … CSA는 제품에 대한 식별, 생산, 검사, 납입, 운영, 유지, 수리, 재장비능력을 향상시킨다.》 CSA는 또한 《한 제품에 대한 력사적인 구성자료원천과 모든 구성문건들을 제공한다.》

이 CSA정보는 제품의 생명주기전반에 걸쳐 알아야 할 필요가 있는 사람들에게 널리 알려 주어야 한다. CSA생명주기문건화의 단계별 실례들은 다음과 같다.

- **개념단계** 요구사항문건들과 그 변화력사
- **정의단계** 세부적인 구성문건들(실례들, 기술설명서, 공학적도안들, 쏘프트웨어설계문건들, 쏘프트웨어이름, 시험계획과 절차)과 그 변화력사와 변경상태
- **구축단계** 보충적인 제품정보(례하면 검증된 구축상태의 단위구성)와 제품변화들과 해당 변량들
- **분배단계** 이 단계의 정보에는 고객들과 납입날자, 설치설정, 담보만기날자, 봉사합의형태와 만기날자가 포함된다.
- **운영단계** 제품의 형태에 따라 그리고 CM책임분담과 관련한 계약합의에 따라 CSA는 달라 질수 있으나 보존된 상태의 제품구성, 수정된 상태의 제품구성, 운영 및 유지보수정보의 수정상태, 변화요청 및 변화통보, 제한조치 등을 포함한다.

- **페기단계** CSA정보는 제품마다 다르며 제품페기가 부정적영향을 가지는가 아닌가 혹은 특정자료의 보유와 관련된 법적 및 계약적법조항이 있는가 없는가에 따라 다르다.

《체계무결성공학》, 정보보안관리편람. 이 장은 사활적인 체계준위의 정보를 기관에 넘겨 주기 위한 구성관리계획이 중요성을 강조하고 있다. 분산된 체계의 CM계획들은 다음의 비용들을 문건에 반영하여야 한다.

- 자료교환의 전반적체계조종을 위한 체계준위 및 싸이트준위방책, 표준, 절차, 책임관계 및 요구사항들
- 매 개인의 싸이트구성의 식별
- 공통의 자료, 하드웨어, 쏘프트웨어
- 매 요소의 구성에 대한 유지보수

공동의 자료와 응용프로그람의 판본을 확인하기 위한 분산조종과 검열사업은 싸이트준위 CM계획들이 분산준위 CM계획들에 종속되여 있는 분산된 체계의 전반에 걸쳐 꼭 같이 진행된다.

변화통계당국(들)은 단일한 부서, 국, 단위들에 의하여 관리되지 않는 분산된 체계에 대한 방책, 기준, 절차, 역할, 책임관계, 요구사항들에 한하여 모든 분산된 체계들과 일치를 이룩할 필요가 있을것이다.

결 론

변화는 불가피하다

기관들에서의 변화는 불가피하다. 하나의 정보체계와 그 직접적환경, 혹은 보다 넓은 기관적환경에서의 변화들은 정보체계의 보안상태의 균형과 실행된 보안해결책들에 영향을 줄수 있으며 또 분명히 줄것이다. 보안에 큰 영향을 줄수 있는 정상적인 기업활동이나 사건들은 다음과 같다.

- 해당 보안상 필요나 대응책을 변경시키는 정보비밀성에서의 사명 및 방책적변화
- 체계보안위험을 증가 혹은 감소시키는 위협변화(례하면 잠재적공격자의 위협동기나 새로운 위협능력들)
- 각이한 보안방식의 운영을 요구하는 응용에서의 변화
- 새로운 보안상공격방식의 발견
- 보안허점의 발생으로 하여 인가를 무효화시킬수 있는 보안파괴, 체계무결성파괴, 비정상적인 정황이나 사고

- 보안상태에 대한 검사, 사찰 혹은 외적인 평가
- 체계구성, 부분체계구성 혹은 요소구성에서의 변화나 질적갱신
- 구성항목의 제거나 품질저락
- 체계공정대응책의 제거나 품질저락(즉 전반보안대안의 사람대면부요구조건 혹은 기타 리론적/절차적구성요소들)
- 그 어떤 새로운 외부적대면부와의 련결
- 운영환경에서의 변화들(례하면 다른 설비나 장소에로의 재배치, 하부시설이나 환경이 제공하는 보호장치에서의 변화들, 외부적인 운영절차에서의 변화들)
- 보안상태를 개선하거나 운영비용을 줄일수 있는 새로운 대응기술의 리용가능성
- 정보체계의 보안인가서의 기한완료

변화는 통제를 받아야 한다

변화에 대한 통제라는 개념의 뒤에는 반드시 변화에 대한 사전승인이 있어야 하며 그 다음에야 변화가 진행된다. 승인을 하자면 변화의 내적의미에 대한 분석이 있어야 한다. 일부 변화들은 정보체계의 보안상태에 부정적영향을 미칠수도 있다. 이미 세워진 계획에 따라 진행하는 CM은 기관들에 여러가지 리익을 가져다 줄수 있는데 그것들은 다음과 같다.

- 완결된 변화효과에 대한 지식에 기초하여 결심채택할수 있다.
- 변화가 필요한 대상이나 실지 리익을 주는 대상들에만 국한될수 있다.
- 제안된 변화들에 대한 분석이 효과적이며 원가를 절약한다.
- 제품정보나 제품구성에 대한 신뢰도가 높아 진다.
- 변화에 대한 정보가 정연하게 통보된다.
- 고객의 리익을 보전한다.
- 체계구성기준선이 추세에 따라 간다.
- 제품대면부에 대한 구성조종을 할수 있다.
- 체계구성과 해당 문건들사이의 일치성이 보장된다.
- 변화후 체계유지보수가 쉽다.

변화통제도 반드시 콤퓨터시설안에서 실행되여야 한다. 매개 콤퓨터시설에는 조작체계, 콤퓨터설비, 망, 환경편의시설(례컨대 공기조화기, 물, 난방, 배관시설, 전기, 경보장치 등)과 응용프로그람들의 변화에 관한 방책이 있어야 한다.

구성관리는 최상의 실천

유럽보안연단은 수년간에 걸쳐 경제의 각 부문에 있는 회사들을 대상으로 체계적인 실례연구를 진행하고 있다. 최근의 한 연구에서는 분산환경에서의 정보기술보안의 조직과 관리문제를 다루었다. 질문을 받은 각기관들의 응답에 의하면 현재 리용되고 있는 체

계들에 대한 변화관리는 보충적으로 연구할 가치가 있는 가장 중요한 보안실천사항에서 6번째자리를 차지하였다. 비록 그 실천사항이 잘 세워 졌으며 모든 응답자들(주로 IT보안관리자, IT관리자, 기능부문의 담당자들임)의 견해에는 매우 중요한것으로 되지만 그들의 의견을 종합하면 다음의 결론이 얻어 진다.

《실례들이 성공적인 경우도 있지만 변화관리는 제일 괜찮은 기관도 개선의 필요성을 느끼는 그러한 분야였다.》

구성관리는 가치부가공정

하나의 공정인 CM이 있음으로 하여 기관들은 그 공정을 자기의 실정에 맞게 리용하여 실정과 환경을 다룸으로써 그 공정에 실현되며 결과물에 가치가 부가되게끔 한다.

이 장을 집필하면서 참고한 수많은 도서들에서 일관하게 강조한것은 이 공정실행에서의 일관성과 이 공정의 반복성에 대한 요구였다. 수많은 활동들을 한두번 일관성없이 실행하는것보다 몇가지 공정들을 일정한 기간에 걸쳐 일관성 있게 반복하는것이 더 좋다. 표준화가 진행되면 그 공정이 차지하는 지위를 알게 된다. 그 공정의 지위와 해당 우점(과 약점)을 알게 되면 그 공정과 그 공정의 산품에 대한 기준선도 생길수 있다. 구성관리를 잘 실행해나가면 능률, 신뢰도, 유지보수도 개선되며 제품의 수명도 길어 지며 개발원가가 적어 지며 위험과 손해부담도 덜어 지게 되며 부족점도 메꾸어 지게 된다. 최상적인 CM실천에 형용사들을 붙여 보자면 《계획적》, 《통합적》, 《일관적》, 《규칙적》, 《작업흐름선에 기초한》, 《유연성 있는》, 《계측적인》, 《투명성 있는》 등을 붙일수 있다.

CM의 보안상 우월성은 예상치 않은 위협요소들과 악성사건들에 대하여 보호하는것이다. CM은 제기된 변화들의 내부관계를 주의 깊게 분석하고 그 변화들을 승인한 다음에야 그것을 실행시켜야 한다. 또한 CM은 필요한 경우(례를 들어 변화가 오유인 경우) 원래구성상태에로 거꾸로 갈수 있는 능력도 가지고 있다(그것은 원래의 구성판들이 문서고에 보관되기때문이다). 일단 검토된 프로그람이 접수되면 프로그람작성자는 변경승인공정을 거치지 않고서는 함정문(trapdoor)을 끼워 넣는것과 같은 악성변경을 하지 못하게 되여 있다.

구성관리실행

구성관리실행에서 보안전문가는 ;

- 건전한 CM방책들에 기초하여 CM활동을 계획하여야 한다.
- 환경조건과 외적조건, 산품의 생명주기, 단계들에 맞게끔 CM공정들을 선택하여야 한다.
- 도구에는 간단한 수동도구, 자동도구 혹은 량자를 결합한 도구도 있을수 있으므로 해당 CM공정에 맞는 도구를 선택하여야 한다.

- 개발과제와 전반적기간에 걸쳐 CM활동들을 일관성 있게 실행하여야 한다.
- CM계획안들을 리용하여 해당 인원들에 대한 강습을 진행할수도 있고 고객, 품질보증인원, 검열자들에게 간단히 설명도 해주어야 한다.
- 기업의 CM을 리용하여 류사한 산품에 대한 완전한 수행계획들의 반복을 피하여야 한다.
- 자원들이 그 과정에 제때에 도움이 되게끔 하여야 한다.
- 보안전문가가 CCB에 참가함으로써 제기된 변경의 보안상 내적관계가 평가되게끔 하여야 한다.
- 변경된 체계를 시험하며 승인을 받은 다음에 전개하도록 하여야 한다.
- 보조부문이나 봉사부문들이 이 변경과정에 도움을 줄수 있게 하여야 한다.
- 구성정보를 체계적으로 기록하고 안전하게 보관하며 승인하여 배포하도록 하여야 한다.
- 주기적인 검열을 진행하여 체계구성과 관련문건(종이문서형식이든 전자문서형식이든)들을 검토확인하여야 한다.

참 고 문 헌

1. The Systems Security Engineering Capability Maturity Model (SSE-CMM) is a collaborative effort of Hughes Space and Communications, Hughes Telecommunications and Space, Lockheed Martin, Software Engineering Institute, Software Productivity Consortium, and Texas Instruments Incorporated.
2. SSE-CMM, Version 2.0, April 1, 1999, p. 2–3.
3. *Ibid.*, p. 22.
4. *Ibid.*, p. 6.
5. *Ibid.*, p. 26.
6. *Ibid.*, p. 31.
7. *Op cit.*
8. SSE-CMM, Version 2.0, April 1, 1999, p. 32.
9. *Ibid.*, p. 38.
10. *Ibid.*, p. 211.
11. *Ibid.*, p. 211.
12. To Fix CM Begins with Proper Training, *ICM Views*, ICM Web site, Institute of Configuration Management, P.O. Box 5656, Scottsdale, AZ 85261-5656, (840) 998-8600, info@icmhq.com.
13. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 9–12.
14. Institute of Configuration Management, P.O. Box 5656, Scottsdale, AZ 85261-5656, (840) 998-8600, info@icmhq.com.
15. *Configuration Management (CM) Resource Guide*, edited by Steve Easterbrook, is available at http://www.quality.org/config/cm-guide.html.
16. *CISSP Examination Textbooks, Volume 1: Theory,* first edition, S. Rao Vallabhaneni, SRV Professional Publications, 2000, p. 135.
17. *Computer Security Basics,* Deborah Russell and G. T. Gangemi, Sr., O'Reilly & Associates, Inc., 1991, p. 146.
18. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 14.
19. *Information Systems Security Engineering Handbook,* Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-48-49.
20. *A Guide to Understanding Configuration Management in Trusted Systems*, National Computer Security Center, NCSC-TG-006, Version 1, 28 March 1988, p. 12, 13.

21. *Op. Cit.*, p. 12.
22. *Information Systems Security Engineering Handbook*, Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-46.
23. AR25-3, Army Life Cycle Management of Information Systems, 9 June 1988, p. 36.
24. BS7799, British Standards 7799, Information Security Management, Part 1, Code of Practice for Information Security Management Systems, 1995, Section 6.2.4.
25. *Computer Security Basics*, Deborah Russell and G. T. Gangemi, Sr., O'Reilly & Associates, Inc., 1991, p. 145.
26. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 18-22.
27. Information Classification: A Corporate Implementation Guide, in *Handbook of Information Security Management*, 1999, p. 344.
28. Information Classification: A Corporate Implementation Guide, in Handbook of *Information Security Management*, 1999, p. 344
29. Systems Integrity Engineering, in *Handbook of Information Security Management*, 1999, p. 634.
30. British Standards (BS7799), Information Security Management, Part 1, Code of Practice for Information Security Management Systems, 1995, p. 19.
31. Ibid., p. 36.
32. British Standards (BS7799), Information Security Management, Part 2, Specification for Information Security Management Systems, 1998, p. 8.
33. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 24–34.
34. FIPS PUB 102, Performing Certification and Accreditation, Section 2.7.3, Change Control, p. 54
35. FIPS PUB 102, p. 9.
36. *Information Systems Security Engineering Handbook*, Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-49.
37. Six Sigma — The Breakthrough Management Strategy Revolutionizing the World's Top Corporations, Mikel Harry and Richard Schroeder, Six Sigma Academy @2000.
38. What is Software CM?, *ICM Views*, ICM Web site, *Op.cit.*
39. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 34.
40. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 35-38.
41. Systems Integrity Engineering, in *Handbook of Information Security Management*, 1999, p. 628.
42. *Information Systems Security Engineering Handbook*, Release 1.0, National Security Agency, Central Security Service, February 28, 1994, p. 3-47.
43. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 23.
44. Systems and Operations Controls, *Handbook of Information Security Management*, 1993, p. 399.
45. Best Business Practice: Organising and Managing IT Security in a Distributed Environment, *European Security Forum*, September 1991, p. 38.
46. EIA-649, National Consensus Standard for Configuration Management, Electronic Industries Alliance, August 1998, p. 11.
47. *Security in Computing*, Charles P. Pfleeger, Englewood Cliffs, NJ: Prentice-Hall, 1989.

제4편
응용 및 체계개발보안

전통적으로 보면 보안통제가 강구되는 곳은 조작체계나 망전반이다. 그러나 무한량의 정보를 처리보관하는 기관 같은데서 정보에 대한 끝없는 요구가 제기됨으로 하여 자료보관고(data warehouse)와 자료시장(data mart)이 우후죽순처럼 생기고 있다. 그러므로 자료기지준위에서의 보안은 더욱 중요하며 자료기지보안기능에 대한 고객의 요구는 점점 높아 지고 있다. 다행스럽게도 일부 주요업체들에서는 자기들의 제품일식내에 세밀통제를 강구할수 있는 기능들을 통합해 넣음으로써 보안요구에 호응하기 시작하고 있다.

인터네트는 사람들이 정보를 다루고 주고받는 방식을 계속 변경시키고 있다. 확장표식언어(XML)와 같은 새로운 고급언어들이 기준으로 되고 있으며 이러한 언어가 있음으로 하여 의뢰기와 봉사기, 대상과 공정간의 운용조작호환성이 약속되여 있는것이다. 이 편에 있는 두개의 장들은 이 언어의 우점들을 남김없이 리용할수 있는 가능성들과 그 단점들에 대하여 고찰하며 독자는 그 도구를 어떻게 하면 잘 리용하면서도 응용보안을 유지하겠는가에 대하여 알게 된다.

인터네트 및 Web관련응용프로그람들을 계속 개발리용함으로써 Web관련프로그람응용코드에 있는 잠재적취약성들을 녹여 낸 실례들을 우리는 많이 보아 왔다. 이 편에서는 Web응용보안실천사항들과 제품에 대한 권고를 다루게 된다. 특히 이 장에서 필자들이 중요하게 강조하려고 하는것은 응용개발속도가 빠르고 시장실현에 대한 긴박성이 매우 높은 최근에 사용자에 대한 교육과 강습이 응용프로그람개발자들에게까지 확대되여야 한다는것이다.

이 편에는 마지막으로 모든 보안개념들을 하나의 완결된 계로 묶어 주는 장이 하나 있다. 필자는 고유한 보안환경을 형성하는 여러 학문들을 탐구하는데서 거시적인것과 미시적인것을 결합시킴으로써 메인프레임시대에 적용되였던 개념들이 새 보안세계질서에 부합되게 하였다.

제27장. Web 응 용 보 안

맨리 앤드리스

요즘 Web상에서 주권시세를 알아 보며 새로운 봉사형태를 청구하며 어느것이나 구매하는 등 거의 모든것을 다 할수 있을가, 누구나 다 하나의 Web응용프로그람을 가지고 있는것 같다. 그런데 정확히 그것이 무엇을 의미할가.

Web응용프로그람들은 구별할수 없는 무한의 프로그람들이다. 여기에는 수많은 각이한 구성요소들과 봉사기들이 들어 있다. Web응용이라고 할 때 여기에는 보통 Web봉사기, 응용봉사기, 자료기지봉사기가 속한다. Web봉사기는 말단사용자를 위한 그래픽사용자대면부를 제공하며 응용봉사기는 업무론리흐름을 제공하며 자료기지봉사기는 응용기능전반에 필요한 자료를 담고 있다.

Web봉사기는 여러가지 각이한 방법으로 응용봉사기에 요구를 보내며 말단사용자에게 변경된 Web페지나 새 Web페지를 다시 보낸다. 이러한 방식들에는 공통관문대면부(CGI: Common Gateway Interface), Microsoft회사의 능동봉사기페지(ASP:Active Server Page), 쟈바봉사기페지(JSP: Java Server Page)가 있다. 일부 경우에는 응용봉사기들로 공통객체요구중개자구조(CORBA: Common Object Request Broker Architecture)와 인터네트객체요구중계자사이규약과 같은 요구중계대면부를 지원하기도 한다.

Web응용보안

모든 응용이 다 창조되거나 실행되거나 동일한것은 아니다. Web응용의 결여는 신속히 최신의 망으로 쉽게 퍼져 나가게 된다. 왜 그런가? Web응용프로그람들은 다 다르면서도 또 다 같은것들이기때문이다. 이것들은 다 같이 꼭 같은 몇개 안되는 Web봉사기상에서 가동하며 꼭 같은 매 점에서 산 쏘프트웨어이며 꼭 같은 응용봉사기와 자료기지봉사기를 리용하나 그 응용프로그람들의 일부라도 자체의 코드를 가지고 있는것으로 하여 서로 다르다. 회사들은 시간적여유나 자원이 부족되여 인터네트로 진출하기전에 자기들이 가지고 있는 봉사기를 충분히 경화시키거나 전면검사해 보지 못하군 한다.

또한 많은 프로그람작성자들은 안전한 응용프로그람을 개발하는 방법을 모르고 있다. 아마 그들은 지금까지 항상 보안상 결점이 발견되여도 큰 파국적결과를 가져 오지 않는 단독응용프로그람들이나 인트라네트Web응용프로그람들을 개발하였을것이다.

결국 많은 Web응용프로그람들은 봉사기, 응용프로그람, 회사에서 개발한 코드들에 취약하다. 그 응용프로그람이 정확히 기능을 수행하려면 포구80(혹은 SSL에는 433)이 열려 있어야 하기때문에 이러한 공백들은 울타리방화벽보안에까지 침투해 들어 온다. Web응용공격들에는 Web응용에 대한 봉사거부공격, Web페지내용바꾸기, 신용카드번호와 같은 회사 및 사용자기밀정보훔치기가 있다.

이 문제점들은 어느 정도 범람하는가. 2000년말의 몇달간에 다음과 같은 이야기들이 뉴스감으로 되였다(이것들은 다 보도에 나온 이야기들이다.). 한 해커는 Egghead.com에 뚫고 들어 와 370만명의 고객들의 구좌들을 열어 놓은것으로 추정되였다. 몇주 지나서야 그 회사는 해커가 고객신용카드번호들에는 접근하지 못했다고 말하였다. 이쯤되면 많은 신용카드번호들이 무효화되고 이 회사의 명성은 이미 손상된것이다. 다른 한 해커는 Creditcards.com에 대한 강탈행위에 나섰는데 그는 이 회사의 싸이트를 뚫고 들어가 5만5천개이상의 신용카드번호를 도적질하였다. 그 해커는 어느 한 Web싸이트에 그 신용카드번호를 게시하고 회사에서 돈을 내면 그것들을 취소하겠다고 하였다. Eve.com의 Web응용프로그람에서 하나의 바그가 생겨 고객들은 URL에서 번호하나만 바꾸면 다른 사람들의 주문을 쉽게 볼수 있었다고 한다. 그 바그는 고객들의 이름과 주소, 제품, 주문날자, 고객들이 쓰는 신용카드형태와 신용카드번호의 마지막 다섯자리수자들을 다 보여 주게끔 되여 있었다. IKEA의 상품명세서주문싸이트의 Web응용프로그람에서는 하나의 바그가 생겨 고객주문정보가 다 로출되였다. 마지막으로 Amazon.com의 Web응용프로그람에 있던 하나의 바그에 의하여 그 많은 고객들의 전자우편주소들이 공개되였다. Web응용프로그람에 의한 공격은 이러한 정도의 위협으로 되여 CERT는 2000년 2월에 이 문제와 관련한 권고안을 발표하였다(표 27－1을 보든가 www.cert.org/advisories/CA–2000–02.html을 찾아 가 보기 바란다).

Web공격이 일반적인 공격과 다른점은 Web공격이 탐지하기 힘들며 그 공격자는 인터네트의 임의의 사용자, 지어는 인증된 사용자로 될수 있다는것이다. 현재까지 이 분야가 상당히 도외시되여 온것은 회사들이 Web공격을 탐지도 못하는 방화벽과 침입탐지장치들을 가지고 자기의 망을 보호하느라고 씨름질하고 있는것과 관련된다.

정확히 Web응용이 공격에 어느 정도로 취약한가. 해커들이 교묘하게 리용할수 있는 점들은 다음과 같다.

- 이미 알려 진 취약점들과 설정오유
- 숨은 마당
- 뒤문선택항목과 오유수정(debug)선택항목
- 싸이트간의 스크립팅
- 파라메터수정
- 쿠키조작
- 입력조작
- 완충기범람
- 직접접근열람

알려 진 취약점들과 설정오유

알려 진 취약점들에는 Web응용에서 사용하는 조작체계들과 제3자적인 응용프로그람에서 나타나는 모든 바그들과 교묘한 점들이 속한다. 가장 널리 사용되는 Web봉사기들의 하나인 Microsoft회사의 Internet Information Server(IIS)는 보안상 결함이 많은것으로 하

여 유명하다. 2000년 10월에 나온 취약점인 Extended UNICODE Directory Traversal취약점(《보안불레찐》MS00–078에서 공개됨》은 IIS가 유니코드(UNICODE)처리를 잘못한것을 교묘히 리용하여 공격자로 하여금 특수한 URL을 입력한후 Web봉사기와 꼭같은 론리적구동장치에 있는 임의의 파일에 접근하게 한다. 공격자는 IUSR–machinename구좌하에 있는 파일들을 쉽게 실행시킬수 있다. IUSR–machinename은 IIS를 위한 닉명의 사용자구좌이며 기정값으로는 Everyone 과 Users Group의 한 성원이다. Microsoft는 이 문제해결을 위한 보강판을 출하하였는데 http://www.microsoft.com/technet/security/bulletin/MS00–078.asp에서 내리적재할수 있다.

이러한 문제들은 설정오유들 즉 불안전한 기정값설정을 가지고 있거나 관리자들에 의하여 불안정하게 설정된 응용프로그람들에도 있다. 그 대표적실례는 임의의 사용자가 한 체계에 있는 디렉터리경로를 제마음대로 넘나들게끔 Web봉사기가 설정된것을 들수 있다. 이렇게 되면 그 Web봉사기에 기밀정보가 있는 경우(이것자체가 큰 보안위험이다) 통과암호나 원천코드, 고객정보와 같은 기밀정보가 루출될수 있다. 다른 하나의 설정오유의 실례는 Web봉사기에서 사용자들에게 실행허가를 주게끔 되여 있는 경우이다. 디렉터리를 넘나 들게 된 경우와 결합되면 이것도 Web봉사기에 손상을 주게 된다.

숨은 마당

숨은 마당은 숨겨 진 HTML양식마당을 말한다. 흔히 여러 응용프로그람에서는 이 마당을 리용하여 체계통과암호나 상품가격들을 표시한다. 이름은 숨은 마당이라고 부르지만 이 마당은 그렇게까지 숨겨 지지 않은것이다. Web페지상의 View Sour를 실행시키면 보일수 있다. 여러 Web응용프로그람에서는 나쁜 사람들이 HTML에 있는 이 마당을 수정하여 상품을 눅은 가격이나 전혀 가격을 물지 않고 구매할수 있게끔 기회를 조성하고 있다. 이러한 공격들이 성공할수 있는 원인은 거의 모든 응용프로그람들이 돌아 오는 Web페지를 확인 혹은 비준하는 체계를 가지고 있지 않는데 있다. 이 응용프로그람들은 돌아 오는 자료가 보냈던 자료와 같을것이라고 전제하는것이다.

뒤문 및 오유수정선택항목

개발자들은 흔히 응용프로그람들에 뒤문을 만들어 놓고 오유수정선택항목을 선택하여 오유퇴치를 쉽게 할수 있도록 한다. 이렇게 하면 개발과정에는 좋은 점이 있지만 인터네트에 올려 놓는 최종프로그람에까지 그대로 이런 항목들이 남아 있게 된다. 사용자들이 통과암호 없이도 접속개시하게 하거나 응용프로그람설정에 직접 접근할수 있는 특별한 URL로 접속개시할수 있는 뒤문들은 아주 인기 있다.

이러한 Web응용프로그람의 취약점이 나타나게 된 원인은 체계운영에서 지켜야 할 규범화된 방책과 절차들이 부족한데 있다. 이 취약점을 처리하기 위한 주요조치는 뒤문을 제거하고 오유수정선택항목의 사용을 금지시키는것이다. 이 단순한 조치를 취하면 응용프로그람의 취약점들이 극력 줄어 들게 된다. 그러나 응용프로그람설치와 기동을 빨리 해야 한다는 요구로 하여 이러한 과정들이 준수되지 못하기때문에 이 단계는 흔히 생략

되군 한다.

싸이트간 스크립팅

싸이트간 스크립팅은 많은 의미를 담고 있기때문에 한마디로 정의하기 어렵다. 일반적으로 싸이트간 스크립팅이란 다른 원천지에서 보내 온 페지들에 코드를 삽입하는 공정을 말한다. 싸이트간 스크립팅은 우선 HTML양식에서 교묘하게 리용될수 있다. 사용자는 이 HTML양식에 그 어떤 정보를 삽입하여 그것을 봉사기에 보낸다. 봉사기는 그 양식에 있는 자료입력내용을 받았다가 그것을 HTML페지로 사용자에게 다시 보내여 그 입력내용을 확인하게 한다. 사용자가 만일 JavaScript프로그람과 같은 코드를 어떤 양식마당에 타자쳐 넣으면 그 페지가 현시될 때 의뢰기열람기가 그 코드를 처리하게 된다.

싸이트간 스크립팅은 신뢰성을 위반하는것으로 된다. 사용자들은 Web봉사기가 보낸 정보를 신뢰성이 있기때문에 그 어떤 나쁜것이 있으리라고 보지 않는다. 그런데 싸이트간 스크립팅을 허용하게 되면 봉사기에 악성코드를 주입하여 그것이 다른 사용자의 콤퓨터에 가서 실행되게 된다. 전자게시판에 게시자료를 투고하는것은 바로 싸이트간 스크립팅의 좋은 실례이다. 바로 이 게시자료에 악성 JavaScript코드를 삽입해 넣는것이다. 어떤 사용자가 그 전자게시판자료를 무심히 접속해서 보는데 그때 바로 봉사기가 HTML을 이 악성코드와 함께 보내여 현시되게 한다. 그러면 Web봉사기가 보내여 온 그것이 타당한 코드인줄 알고 그 사용자의 열람기는 코드를 실행시킨다.

파라메터수정

파라메터수정이란 사용자가 보지 말아야 할 정보를 검색할 목적으로 URL렬을 함부로 조작하는것을 말한다. URL에 포함되여 있는 SQL호출신호를 통하면 Web응용프로그람의 후위자료기지에 접근할수 있게 된다. 사용자가 나쁜 마음을 먹게 되면 이 SQL코드를 조작하여 그 자료기지에 보관된 모든 사용자명단, 그들의 통과암호, 신용카드번호 등을 검색해 낼수 있게 된다. 앞에서 언급한 Eve.com의 결함은 바로 이러한 파라메터수정의 결과였다.

쿠키조작

쿠키조작이란 쿠키에 담겨 진 자료를 수정변경하는것을 말한다. Web싸이트들은 사용자 ID, 통과암호, 구좌번호 등을 포함한 사용자콤퓨터에 대한 쿠키들을 보관한다. 나쁜 마음을 먹은 사용자는 이 쿠키들을 못쓰게 하거나 변경시켜 자기것이 아닌 남의 구좌들에 접근할수 있게 된다.

또한 공격자들이 사용자들의 쿠키들을 도적질하여 구좌들에 접근할수 있다. Web전자우편이나 직결은행과 같은 Web응용에서는 흔히 쿠키자료를 리용하여 사용자인증을 한다. 만일 해커들이 쿠키에 접근하여 그 쿠키를 자기의 열람기에 끌어 오면 사용자ID

와 통과암호를 입력하지 않고 혹은 다른 형태의 인증을 하지 않고도 사용자구좌에 접근할수 있게 된다. 구좌접근은 대화가 진행되는 동안에만 (Web응용프로그람들이 대화시간경과를 규제하고 있으므로) 가능하지만 손해는 이미 다 본것이나 다름없다. 몇분이면 공격자는 쉽게 남의 은행구좌를 깡그리 털고 은행총재를 위협하는 전자우편을 보낼수 있게 된다.

입력조작

입력조작이란 CGI스크립트로 처리되는 HTML양식입력사항들을 조작하여 체계명령을 실행시키는것을 말한다. 실례로 CGI를 사용하여 다른 사용자에게 정보를 보낼수 있는 양식의 입력자료를 조작하여 봉사기에 있는 통과암호파일을 자기에게 끌어 오거나 그 봉사기에 있는 모든 파일들을 다 지워 버릴수도 있다.

완충기범람

완충기를 범람시키는것은 악성사용자가 굉장한 량의 자료를 봉사기에 보냄으로써 봉사기를 굳어 지게 하는 고전적인 공격기법이다. 봉사기에는 완충기가 있어 여기에 이 자료들을 받아 기억한다. 받은 자료가 완충기용량보다 큰 경우에는 탄창기억이 자료의 어떤 부분들로 꽉 차게 된다. 만일 이 자료가 프로그람코드이면 체계는 그 탄창기억에 꽉 차 있는 임의의 코드를 실행시킬것이다. Web응용프로그람완충기범람공격의 실례는 이 경우에도 HTML양식을 리용하는것이다. 양식의 어떤 마당에 들어 가 있는 자료가 너무 크면 이것도 역시 완충기의 범람조건으로 될수 있다. 특별히 기형적으로 된 양식자료가 있으면 봉사기가 임의의 코드를 실행하게 되여 공격자로 하여금 그 체계에 대한 조종권을 완전히 장악할수 있게 할수도 있다.

완충기범람에 관하여 더 알려면 http://www.cultdeadcow.com/cDc–files/cDc–351/에서 Dildog가 쓴 "Tao of a Buffer Overflow"라는 책을 보면 된다. 기타 참고서들로서는 http://www2.linuxjournal.com/lj–issues/issue61/2902.html에 있는 "A Look at the Buffer–Overflow Hack" 그리고 http://www–miaif.lip6.fr/willy/security에 있는 "UNIX Security: The Buffer Overflow Problem"을 들수 있다.

직접접근열람

직접접근열람이란 인증을 거쳐야 할 Web페지에 직접 접근하는것을 말한다. Web응용프로그람들이 제대로 설정되여 있지 않는 경우 악성사용자들은 기밀정보가 담겨 진 URL들에 직접 접근할수 있으며 만일 값을 내고 보아야 하는 경우 회사에 재정적손실을 줄수 있다.

Web응용프로그람에 대한 공격은 각 회사의 자산, 자원, 명성에 막대한 손실을 줄수 있다. Web리용에서 공격위험이 증가되기는 하지만 이 위험을 완화시킬수 있는 해결책들은 많다.

예 방

Web응용공격들을 예방할수 있는 최선의 방도는 교육을 주고 경각성을 높이는것이다. 개발자들에게는 안전한 코드화과정에 대한 교육을 주며 경영측에는 충분한 시험과정을 거치기전에 어떤 체계를 가동시킬 때 생길수 있는 위험성에 대하여 충분히 알려 주어야 한다. 또한 관리자들과 보안전문가들은 판매업체의 Web싸이트, 보안Web싸이트, 보안우편관계목록 등을 항시적으로 감시함으로써 Web응용프로그람들과 봉사프로그람들에 새로운 취약점들이 나타나지 않았는가를 알아 내야 한다. 우수한 정보를 제공하는 최상의 보안싸이트들로서는 securityfocus.com, securityportal.com, ntsecurity.com, linuxsecurity.com 등을 들수 있다. 회사나 기관자체로 개발한 응용프로그람들이 얼마나 안전한가에는 관계없이 공격자들은 자료기지봉사기에 있는 하나의 취약점을 뚫고 들어와 모든것을 다 접근할수 있다.

개발자들에 대한 교육에서 첫째도 둘째도 셋째도 중요한것은 그들이 들어 오는 자료는 절대로 믿지 않게 하는것이다. 말단사용자들을 믿기 어려우므로 안전한 Web응용프로그람을 만들기까지는 많은 시간이 필요하게 된다. 개발자들은 오직 자기가 통제나 조종할수 있는것만 믿어야 한다. 말단사용자에 대한 통제를 할수 없으므로 개발자들은 들어오는 모든 자료들은 다 위험한것으로 가정하지 않으면 안된다. 사용자열람기로 보냈던것이 변하지 않고 되돌아올것이라고 생각하거나 Web양식에 입력된 자료가 정확하다고 가정하는 일이 절대로 있어서는 안된다. 고객주소를 적어 넣어야 할 양식에 《<》기호가 하나 꼭 있어야 될가. 이러한 기호는 흔히 코드를 가리킨다. 려파기를 추가하거나 입력검사를 하면 Web공격의 대부분을 확고히 제거할수 있다.

개발자들은 또한 코드화과정에 그 응용프로그람에 모든 보안대책들을 다 포함시켜야 한다. 물론 매 사용자가 자기 이름과 통과암호로 인증을 받고 그 응용프로그람에 접근하겠지만 개발과정에 시간을 절약한다고 하면서 개발자들이 닉명으로 Web봉사기구좌를 사용한다면 일련의 골치거리가 생길수 있다. 례를 들어 인증코드에 바그가 있어도 그 응용프로그람을 완성하기 며칠전에 혹은 완성후에야 발견되는 경우도 있을수 있다. 마지막순간에 바그를 발견한다는것은 그 응용프로그람의 봉사개시가 늦어 지거나 바그가 있는 채로 봉사를 개시한다는것을 의미한다. 이 두 경우 다 위험하므로 개발공정의 전반에서 모든것을 다 포함시켜 고려해야 한다.

가능하면 관리자구좌나 운용관리자(superuser)구좌를 리용하지 말고 응용프로그람을 가동시켜야 한다. 뿌리준위에서 모든것을 가동시키는것이 접근하는데 시간절약하는것같이 생각되지만 그렇게 하면 화를 스스로 청하는것으로 된다. 운용관리자구좌로 모든것을 가동시키면 Web응용프로그람사용자는 누구나 다 자료기지표에 완전한 쓰기접근을 할수 있게 될것이다. 악성사용자는 SQL코드로 몇가지 URL들을 수정하기만 하면 자료기지전부를 쉽게 지워 버릴수 있다. 특권의 최소화라는 보안방책을 준수하는것이 최상의 방책이다. 특권의 최소화란 사용자에게 해당 과제를 수행하는데 필요한 최소수준의 허용사항들을 주는것을 말한다. 그렇게 해도 사용자는 Web을 잘 리용하며 회사는 회사대로 사용자접근이 제한되였으니 비법적인 행위들이 크게 없을것이라고 안심하니 좋을것이다.

HTTP GET요구신호를 리용하여 의뢰기로부터 봉사기에로 기밀자료를 보내게 되면 여러가지 보안허점들이 생기므로 이것을 피해야 한다. 이 GET요구신호는 Web봉사기사용기록부에 평문으로 등록되므로 누구나 다 읽어 볼수 있다. 이러한 GET요구신호로 봉사기에 전송된 신용카드번호도 Web봉사기사용기록부에 평문으로 등록되여 있게 된다. 공격자가 Web봉사기사용기록부에 접근하기만 하면 자료기지암호화를 리용하여 신용카드번호를 보호하려고 해도 소용 없다. SSL도 역시 이 문제를 예방하지 못한다. SSL은 전송과정에만 자료의 암호화를 보호하므로 GET요구신호는 이때에도 Web봉사기에 평문으로 기록되게 된다. 이 GET요구신호는 또한 고객열람기의 리력파일에도 보관될수 있다.

그러므로 의뢰기와 Web봉사기사이의 자료전송에는 HTTP POST명령을 사용해야 한다. POST명령은 HTTP를 리용하여 정보를 넘기므로 Web봉사기에 그 사용기록이 남아있지 않게 된다. 정보는 그래도 평문으로 보내여 지므로 SSL을 리용하여 망에서의 엿보기공격을 막아야 한다.

JSP와 ASP(*SP)는 흔히 Web응용프로그람개발에 리용되는데 흔히 디렉터리, 자료기지 등에 접속할수 있는 수정불가능하게 된 통과암호를 가지고 있다. 일부 사람들의 생각에는 봉사기가 그 코드를 처리하여 그 결과물로 Web페지를 현시하므로 좋다고 할수 있지만 언제나 그렇게 되지 않으므로 수많은 취약점들이 있다. 이것을 증명할수 있는 가장 간단한 해커기법으로서는 IIS바그인데 ::$DATA가 어느 한 URL의 끝에 붙었을 때 이 IIS바그로 하여 ASP의 원천코드를 볼수 있게 된것도 그 실례이다. 례를 들어 http://www.site.com/page.asp::$DATA를 주면 그 페지의 원천코드와 거기에 담긴 짭짤한 비밀까지 현시될수 있다.

개발자들은 정보를 루출시킬수 있는 HTML코드주석과 오유경고문에 대해서도 언제나 인식을 잘하여야 할것이다. 이것들이 직접 공격을 유발시키지는 않으나 공격자는 이것을 보고 그 응용프로그람의 구조를 충분히 알아 내여 공격을 성과적으로 단행할수 있을것이다. 실례로 봉사기의 스크립트의 일부였던 접속문자렬이 주석에 포함되여 나타나면 공격자는 귀중한 정보를 얻는것으로 된다.

오유경고문도 주의해야 할 필요가 있다. 일부 오유경고문들은 Web봉사기의 물리적경로에 대한 정보를 알려 주므로 그것이 Web봉사기공격에 리용될수 있다. 일부 오유경고문들은 현재 사용중에 있는 해당 자료기지봉사기나 응용프로그람봉사기에 대한 정보를 로출시킬수 있다. 총괄해 보면 오유경고문들은 그 어떤 특정한 위험을 일으키지 않지만 이 경고문들에서 조금씩 수집한 정보를 리용하여 응용프로그람의 구조를 알수 있으며 공격에 대한 세밀한 준비를 할수 있다.

싸이트간 스크립팅은 물리치기 힘든 매우 효과가 높은 공격이다. 현재 일치한 의견을 본 해결책은 HTML부호화를 리용하는것이다. HTML부호화에서는 《<》과 《>》와 같은 특수부호들에 설명어가 할당된다. <는 &1t이고 >는 >이다. 부호화된 문자는 열람기에 보내지면 실행되지 않고 현시된다. 앞에서 설명한 전자게시판공격같은것들을 예방하자면 입력자료들이 부호화되여야 한다. 일부 제품들에는 이것을 위한 도구가 포함되여 있다. 실례로 IIS에는 Server항목에 HTMLEncode가 있으므로 여기서 입력문자렬을 받아 자료를 부호화된 형식으로 출력해 준다.

안전한 부호화는 안전한 Web응용프로그람개발에 필요되는 여러 내용들중의 하나에 불과하다. 리상적으로 보건대 보안을 응용프로그람개발의 전과정에서 토론되고 계획화되고 포함되여야 할 문제인것이다. 이렇게 되는 경우 최종결과물인 Web응용프로그람은 진정으로 안전하고 공고한것으로 될것이다. 또한 Web응용프로그람을 계속적으로 감시, 보수할수 있는 절차들이 마련되여야 그 응용프로그람의 보안이 유지될것이다.

기술도구와 해결책

안전한 부호화과정이 안전한 Web응용프로그람을 낳게 하지만 이것만으로는 충분하지 못하다. Web응용프로그람을 검열하고 안전하게 할수 있는 도구들과 응용프로그람들은 여러가지가 있다.

Web응용프로그람이 CGI스크립트를 사용한다면 RFP(제한의뢰서)에 있는 whisker.pl스크립트를 가지고 그 응용프로그람을 스캔할수 있다. 이 Perl스크립트는 알려 진 CGI취약성들을 알아 보기 위하여 싸이트를 스캔한다. 이 스크립트는 www.wiretrip.net/rfp에서 무료로 구입할수 있다.

원천코드를 철저히 검토해 보는것도 매우 중요하다. 전문가를 한명 고용하여 전반적으로 검토하는것은 비용이 상당히 들지만 이 과정을 기관내에서 진행할수 있는 프로그람도 여러가지가 있다. NuMega(www.numega.com), L0pht(www.l0pht.com/slint.html), ITS4(www.rstcorp.com/its4), Lclint(lclint.cs.virginia.edu)들은 모두 원천코드검토프로그람들을 제공한다.

몇가지 제품들은 Web응용보안에 특효가 있다(그 제품들의 수는 급속히 늘어 나고 있다). Sanctum회사의 AppShield제품(www.Sanctuminc.Com)은 이 장에서 언급된 모든 취약점들이 Web싸이트에서 제기되지 않게 해준다. AppShield는 Web응용프로그람을 위한 방화벽처럼 작용함으로써 승인된 자료와 승인된 요구신호만 그 Web응용프로그람에 넘어가도록 해준다. 이 회사에는 또한 응용프로그람들의 취약점을 검사하는데 쓰이는 AppScan도 있다.

S.P.I.Dynamics회사(www.spidynamics.com)의 Webinspect응용프로그람은 Web페지, 스크립트, 고유독점코드, 쿠키 등 Web응용취약점들을 찾아 준다. WebDefend는 Sanctum회사의 AppShield처럼 Web응용공격들에 대한 실시간 탐지, 경고, 반응을 진행한다.

시장에 나돌고 있는 몇가지 다른 제품들도 일부 Web공격으로부터 Web응용프로그람들을 보호할수 있다. Encercept와 원천공개형인 Saint Jude는 새로운 침입방지응용프로그람으로서 공격이 진행되기전에 조작체계의 준위에서 공격을 저지시킨다. 이 제품들은 조작체계준위에서 완충기범람공격이나 싸이트간 스크립팅을 저지시켜 Web응용프로그람을 보호할수 있다. 또한 SecureWave회사에서 출품한 SecureStack (http://www.securewave.com/html/secure_stack.html)은 Windows NT와 Windows 2000을 사용하는 봉사기들에서 완충기범람을 막는다.

요 약

Web응용프로그람들에 있는 빈 구멍들을 리용하는것은 순식간에 봉사기와 거기에 있는 기밀정보들에 대한 접근을 할수 있는 좋은 공격방법으로 된다. 판매업체들에서 제공하는 응용프로그람이든 회사자체안에서 만든 프로그람이든 거기에는 공격자가 보지 말아야 할 정보를 읽어 보며 지어 그 체계전반을 장악할수도 있는 여러가지 방법이 있다.

이러한 빈 구멍들이 있게 되는것은 프로그람작성자들과 응용개발자들이 안전한 프로그람기법에 대한 교육을 옳바로 받지 못한것과 관련된다. 정확히 교육을 받았다고 하는 사람들도 빈 구멍들을 제대로 막는 작업을 빈틈없이 하지 못하고 있는데 그 원인은 제품의 시장실현기일에 대한 촉박감으로 하여 그 응용프로그람들의 안정성을 정확히 보장할만한 시간적여유가 없기때문이다.

Web응용프로그람들에 있는 주되는 보안상구멍들에는 알려 진 취약점들, 설정오유, 숨은마당, 뒤문 및 오유수정선택항목, 싸이트간 스크립팅, 파라메터수정, 쿠키조작, 입력조작, 완충기범람, 직접접근열람이 있다.

이러한 취약점들로부터 응용프로그람들을 보호하자면 개발자들에 대한 교육이 관건적이다. 또한 취약점들을 발견하고 응용프로그람들이 이러한 취약점들로 하여 해커공격을 받지 않게 보호할수 있는 몇가지 판매되는 도구들과 제품들도 중요하다.

결론적으로 말하여 Web응용프로그람들에 대한 공격들은 나날이 급속히 증가되는 위험이라고 말할수 있다. 이러한 Web응용프로그람에 의하여 전 세계의 누구에게나 다 접근가능한 자료들과 자원들을 보호하는데서 관건적역할을 하는것은 교육과 경각성이다.

표 27-1 콤퓨터비상대응팀(CERT)정황보고CA-2000-02 의뢰기 Web요구신호에 삽입된 악성HTML태그

이 정황보고는 CERT조정쎈터, 국방성(DoD)CERT, DoD콤퓨터망방위를 위한 합동특별수사대(JTF–CMD), 련방콤퓨터사건대응본부(FedCIRC), 전국기반시설보호쎈터에서 공동으로 발표되고 있다.

원본발행날자 : 2000년 2월 2일

최종수정날자 : 2000년 2월 3일

해당되는 체계들

- Web열람기
- 미확인입력사항에 기초하여 Web페지를 동적으로 생성시키는 Web봉사기들

개 괄

Web싸이트는 신뢰성이 없는 원천에서 온 미확인입력내용에 기초하여 동적으로 생성된 페지에 악성 HTML태그나 스크립트를 부정적으로 담고 있을수 있다. 생성된 페지가 정확히

코드~~화되~~여 필요 없는 스크립트실행을 하지 않도록 Web봉사기가 정확히 담보되지 않은 경우 그리고 악성 HTML이 사용자에게 제시되지 않도록 입력사항이 승인되지 않는 경우 문제가 제기될수 있다.

Ⅰ. 해설

배 경

대부분의 Web봉사기들은 자기로부터 내리적재한 Web페지에 포함된 스크립트들을 해석하는 기능들을 가지고 있다. 이러한 스크립트들은 여러가지 스크립트작성언어로 씌여 져 의뢰기의 열람기들에 의하여 실행된다. 설치된 대부분의 열람기들에는 기정값으로 된 설정된 스크립트실행능력이 있다.

한 의뢰기로부터 다른 의뢰기로 보내는 악성코드

Web대면부를 가지고 토론그룹을 운영하는 싸이트들은 한 의뢰기가 다른 의뢰기에 보내는 통보문에 악성HTML태그를 포함시키는것과 같이 취약점을 가지지 않도록 오랜 기간 보호대책을 취해 왔다. 실례로 공격자는 다음과 같은 통보문을 보낼수 있다.

```
Hello message board. This is a message.
<SCRIPT> malicious code </SCRIPT>
This is the end of my message.
```

열람기에서 실행가능으로 된 스크립트들을 받은 피해자가 이 통보문을 읽어 보는 순간 그 악성코드는 예견치 않게 실행될수 있다. 이런 식으로 포함된 스크립트작성태그들에는 <SCRIPT>, <OBJECT>, <APPLET>, <EMBED>가 있다.

의뢰기들사이의 통신이 봉사기를 거쳐서 진행될 때 입력자료가 다른 사용자들에게 보내여 지면 싸이트개발자들은 그 입력자료가 믿지 못할것이라는것을 명백히 알아차리게 된다. 대부분의 토론그룹봉사기들은 이러한 입력을 접수하지 않든가 혹은 그것을 코드화/려과한 후에야 다른 의뢰기들에 넘긴다.

한 의뢰기가 실수하여 자기에게 다시 보내는 악성코드

한 의뢰기가 악성코드를 보내는데 그것이 자기에게 다시 와서 사용될수 있다는 가능성에 대해서는 많은 인터네트Web싸이트들이 보지 못하고 있다. 이것은 쉽게 생길수 있는 실수이다. 그렇다면 왜 한 사용자는 자기가 볼 악성코드를 입력하겠는가.

그러나 그 사용자가 신뢰성 없는 정보원천에 기초하여 청구서를 제출할 때에는 이런 경우가 생기는 법이다. 실례로 공격자는 다음과 같은 악성코드를 구축할수 있다.

```
<A HREF=“http://example.com/comment.cgi?
mydocument=<SCRIPT> malicious code </SCRIPT>”> click
here </A>
```

어떤 사용자가 무심히 이 련결을 딸깍하면 example.com으로 보낸 URL에 악성코드가 포함된다. 만일 Web봉사기가 mydocument의 값을 포함하여 한 페지를 그 사용자에게 보내는 경우 그 의뢰기에서 그 악성코드가 예상치 않게 실행될수 있다. 이런 경우는 전자우편통보문이나 뉴스그룹통보문에 붙어 있는 신뢰성없는 련결점들에서도 일어 난다.

기타 태그들의 악용

스트립트작성태그뿐아니라 <FORM>태그와 같은 HTML태그도 공격자가 악용할 가능성이 있다. 실례로 악성 <FORM>태그를 정확한 곳에 넣음으로써 공격자는 사용자들을 속여 현존양식의 행동방식을 수정케 하여 기밀정보를 루설시키게 할수 있다. 기타 HTML태그들도 악용하면 페지모양을 달리 할수도 있고 바라지도 않거나 기분에 거슬리는 영상이나 음성을 삽입할수도 있고 페지의 기존모습이나 행동방식을 다른 방법으로 방해를 놓을수도 있게 된다.

신뢰성악용

주되는 신뢰악용에서 기본적인것은 example.com싸이트의 보안환경내에서 《주입된》 스크립트나 HTML이 기동케 함으로써 신뢰성을 다 훼손시키는것이다. 신뢰성있다는 싸이트이므로 열람기사용자들이 믿음을 가지고 방문하고 거래하고 싶어 하다가 문제가 제기되는것이다. 또한 합법적인 봉사기싸이트 example.com의 보안방책도 짐작컨데 금이 간 방책일수 있다.

다음의 실례는 두개의 싸이트가 개입되였다는것을 명백히 보여 준다.

```
<A HREF="http://example.com/comment.cgi?
mydocument=SCRIPT SRC='http://bad–site/badfile'></
SCRIPT>"> click here </A>
```

<SCRIPT>태그안에 있는 SRC속성이 비법원천(bad–site)에서 오는 코드를 명백히 내포하고 있다는것을 류의해야 한다. 앞에서 언급한 두 실례들은 다음의 스크립트작성보안모형에서 근본적인 동일원천출발방책이 위반되였음을 보여 준다.

- Netscape Communicator 동일원천방책
- Microsoft Scriptlet 보안

한 원천이 다른 원천에서 받은 페지에 코드를 주입해 넣는것으로 하여 이 취약성도 역시 싸이트간 스크립팅이라고 부른다.

본정황보고가 발표될 때까지 이 취약성을 교묘하게 리용한 사건들이 CERT/CC에 보고된 적은 없었다. 그러나 이 취약성을 리용할 위험성은 있으므로 우리는 각 기관들의 정보총괄책임자들, 리사들, 체계행정관리자들에게 이 문건의 해결책부분에 지적된 조치들을 무조건 강행할것을 권고하는바이다. 해당한 기술기관들, 운영기관들, 사법기관들에 기술적의견을 적극 제기하기를 바란다.

Ⅱ. 영향

사용자들이 Web페지, 우편통보문, 뉴스그룹알림문들에 있는 신뢰성없는 련결점들을 따라 가는 경우 공격자가 써넣은 스크립트들이 예견치 않게 실행될수 있다. 또한 다른 사용자가 제공한 내용에 기초한 동적으로 생성된 페지들을 보는 경우 악성스크립트들이 사용자도 모르게 실행될수도 있다.

악성스크립트들이 마치도 사용자가 목적했던 싸이트에서 온것처럼 보이는 상태에서 실행되기때문에 공격자는 검색된 문건에 대한(공격자가 쓰는 기술에 따라) 완전한 접근을 가지며 페지에 포함되여 있는 자료들을 원래싸이트에 돌려 보낼수도 있다. 실례로 악성스크립트는 실지의 봉사기가 제공한 양식에 있는 마당들을 읽은 다음 이 자료를 공격자에게 보낼수 있다.

문서객체모형(DOM)에 대하여 공격자가 어느 정도로 접근하는가 하는것은 그 공격자가 선택한 언어의 보안구조에 달려 있다. 구체적으로 보면 JavaApplet들을 가지고는 공격자가 DOM에 접근할수 없다.

또한 공격자는 합법적Web봉사기와의 보충적인 교제를 피해자가 모르게 진행하는 스크립트도 삽입할수 있다. 실례로 공격자는 교묘한 수를 개발하여 합법적Web봉사기의 다른 페지에 자료를 투고하였다. 또한 피해자의 Web열람기가 스크립팅을 지원하지 않는다고 하여도 공격자는 페지의 모양새를 고치거나 그 행동방식을 수정하거나 기타 방법으로 정상적인 운영을 방해할수도 있다.

구체적인 영향은 공격자가 선택하여 리용하는 언어와 공격을 받게 되는 해당 합법적페지의 설정값들에 따라 크게 달라 질수 있다. 인차 발견하기 힘든 일부 경우들을 보면 다음과 같다.

SSL암호접속이 로출될수 있다.

안전소케트층(SSL)암호화접속이 의뢰기와 봉사기사이에 이루어 지기전에 악성스크립트 태그가 들어 간다. SSL은 이 선로로 보내여 지는 자료를 악성코드도 포함하여 암호화하며 이것은 두 방향으로 보내여 진다. 의뢰기와 봉사기사이의 통신을 누가 훔치지 않는다고 보면서 SSL은 전송된 자료의 합법성을 확인하려고 하지 않는다.

의뢰기와 봉사기사이에 실지 합법적인 대화를 하므로 SSL은 그 어떤 문제점에 대한 보고도 하지 않는다. 비SSL URL에 접속하려는 악성코드는 불안전한 접속에 대하여 경고문을 발생시킬수도 있으나 공격자는 SSL능력이 있는 Web봉사기를 가동시킴으로써 이 경고가 나오지 않게 할수 있다.

쿠키조작을 통하여 공격이 지속될수 있다.

합법적Web싸이트에서 온 악성코드가 일단 실행되고 있으면 쿠키가 조작되여 공격이 지속될수 있다. 구체적으로 보면 만일 취약성이 있는 Web싸이트가 페지들을 동적으로 생성하는데서 쿠키로부터 온 마당을 리용한다면 공격자는 그 쿠키를 조작하여 거기에 악성코드를 포함시킬수 있다. 그러면 그 쿠키를 그 싸이트가 요구하여 거기에 있는 악성코드를 포함한 마당을 가진 페지를 현시하는 경우 그 Web싸이트를 계속 방문하게 되면 많은 손해를 가져 올수 있다.

공격자가 의뢰기로부터 제한성Web싸이트에 접근할수 있다.

공격자는 악성URL을 만들어 어느 한 의뢰기콤퓨터상에서 스크립트코드를 실행시킬수 있다. 이때 그 콤퓨터는 자기가 속한 인트라네트에 있는 어떠한 취약한 봉사기로부터 자료를 꺼낼수 있는 콤퓨터이다.

공격자는 타개된 그 의뢰기가 인트라네트Web봉사기에 대하여 인증되였으면 그 봉사기에 비법Web접근을 할수 있게 된다. 공격자가 그 어떤 특정한 체계로 가장할 필요도 없다. 공격자는 다만 취약성이 있는 인트라네트봉사기만 알아 내고 그 인트라네트봉사기에 있는 기밀자료를 꺼낼수 있는 무심히 보이는 어느 한 페지를 사용자가 방문하도록 설유하기만 하면 된다.

령역위주의 보안방책이 위반될수 있다.

사용자의 열람기가 일부 호스트나 령역에서 오는 스크립트작성언어들이 실행되게 하면서도 이런 특권을 남들이 가지지 못하게끔 설정되였다면 공격자들은 이것을 리용할수 있다.

공격자는 스크립트실행능력이 있는 봉사기에 보내는 요구신호에 악성스크립트태그들을 삽입함으로써 자기도 이러한 특권적접근을 가지게 된다. 실례로 Internet Explorer의 보안《지대》들이 이 기법에 의하여 전복될수 있다.

흔히 쓰지 않은 문자모임을 사용하면 추가적인 위험이 있을수 있다.

Web봉사기가 돌려 보낸 페지에 문자모임이 지정되지 않은 경우 열람기는 자기가 받은 정보를 사용자가 지정한 문자모임으로 해석한다. 그러나 많은 Web싸이트들은 (ISO–8859–1에 있는 특수한 의미를 가진 문자들을 코드화하거나 려파하는 경우에조차)문자모임을 명백히 지정해 주지 못하여 자기의 문자모임을 쓰는 사용자들을 위험에 빠뜨리게 된다.

공격자는 양식들의 행동방식을 고쳐 놓을수 있다.

어떤 조건하에서 공격자는 결과를 제출하는 방식을 비롯한 양식들의 행동방식을 수정할수도 있을것이다.

Ⅲ. 해결방도

사용자가 알아야 할 해결방도

Web사용자들이 취할수 있는 해결방도에는 완성된 해결방도란 하나도 없다. 이런 류형의 문제점들을 없애기 위해서는 Web페지개발자들이 자기들이 만드는 페지들을 수정하는것이 기본이다.

그러나 Web사용자들이 이러한 공격들을 받지 않게 하려면 두가지 기본적인 선택안들이 있다. 첫째안인 열람기에서 스크립트작성언어를 기능정지(disable)시키는것이 가장 좋은 보호대책이나 일부 중요한 기능들을 정지시킴으로써 부정적작용이 있게 된다. 사용자들은 위험을 최소수준으로 유지해야 할 필요성이 있는 경우에만 이 선택항목들을 설정하여 쓸수 있다.

두번째안 즉 처음으로 방문하는 Web싸이트들은 어떤 방법으로 방문하겠는가를 선정해 주는것은 기능들을 정지시킴이 없어도 위험을 훨씬 약화시킬수 있다. 여기서 사용자들이 알아야 할것은 이 경우 더 많은 위험요소들이 있으나 그렇게 설정하는것은 중요한 기능들을 보

존리용하기 위해서라는것이다.

그렇지만 이 두가지 해결안들사이의 위험상차이를 량적으로 측정하기는 불가능하다. 스크립트언어의 실행가능(enabled)상태로 열람기를 계속 쓰려는 사용자들은 정기적으로 CERT/CC의 Web싸이트들을 재방문하여 갱신판을 받아야 할뿐아니라 이러한 위험성이나 위협요소들이 얼마나 증가하는가에 대하여 다른 보안정보원천들도 조회하여 알아야 할것이다.

Web사용자는 열람기의 스크립트언어의 기능을 정지시켜야 한다.

이 취약성을 교묘하게 리용하여 코드를 실행시키자면 일정한 형태의 삽입된 스크립트언어가 피해자의 열람기에서 실행가능으로 설정되여야 한다. 모든 스크립트언어들을 실행불가능하게 하면 이 취약점의 가장 중요한 영향이 제거될수 있다.

그렇지만 공격자들이 다른 HTML태그들을 URL에 삽입하는 방법으로 합법적싸이트에 의하여 제공되는 내용의 모습에 영향을 줄수도 있다는것을 알아야 한다. 스크립트언어를 실행불가능하게 하여도 <FORM>태그의 악성사용은 막지 못한다.

당신의 열람기에서 스크립트언어를 실행불가능하게 하는 구체적인 지시사항들은 우리의 Malicious Code FAQ(악성코드 질문봉사)에서 받아 볼수 있다(홈페지주소: http://www.cert.org/tech–tips/malicious–code–FAQ.html).

Web사용자는 무질서한 열람을 하지 말아야 한다.

일부 사용자들은 스크립트언어를 완전히 실행불가능하게 할줄 모르거나 그렇게 하려 하지 않는다 . 이 스크립트실행불가능이 가장 효과적인 방안이기는 하지만 일련의 기법들을 리용하면 사용자가 이러한 취약성에 빠지는것을 줄일수 있다.

싸이트간 스크립팅이 가장 위험한것이므로 사용자들은 해당 Web싸이트의 첫방문을 잘 가려서 선정하면 일정한 보호상태를 얻을수 있다. 열람에 직접 주소를 타자쳐 넣는것(혹은 안전하게 보관된 현지 북마크(bookmark)를 리용하든가)은 싸이트접속의 가장 안전한 방도이다.

중요치 않은 싸이트들에 접근하는 경우에도 그 망의 다른 국부체계들에도 접근할수 있는데 그런 경우는 의뢰기체계가 방화벽뒤에 위치하고 있는 경우 혹은 그 의뢰기가 다른 Web봉사기(례를 들면 인트라네트의 봉사기)들에 접근할수 있는 신원내용들을 캐쉬에 보관하였던 경우들이 있다. 그렇기때문에 주의하여 Web싸이트들을 열람하는것은 스크립트실행불가능보다 못하다.

스크립트가 실행가능으로 선택된 경우 눈으로 련결점들을 조사해 보아도 악성련결점을 따라 가지 않을수가 없다. 그것은 공격자의 Web싸이트가 사용자창에 나타나는 그 련결점들을 허위적으로 대표하게 하는 스크립트를 리용하기때문이다. 실례로 Netscape의 Goto와 Status띠의 내용들이 JavaScript로 조종될수 있다.

Web페지개발자들과 Web싸이트관리자들이 알아야 할 해결방도

Web페지개발자들은 동적으로 생성되는 페지들을 재코드화하여 출력을 확인해야 한다.

Web싸이트관리자들과 개발자들은 자기들의 싸이트들이 이러한 취약성으로부터 산생되

는 악용의 영향을 받지 않게 하려면 동적으로 생성되는 페지들에 필요 없는 태그들이 포함되지 않도록 하여야 한다.

입력흐름에서 위험한 메타문자들을 제거해 버리려고 해도 많은 위험요소들이 처리되지 않은채로 남아 있게 된다. 우리는 페지작성에 사용되는 변수들을 명백히 허용된 문자들로 제한시킬것과 출력페지의 생성과정에 이 변수들을 검사해볼것을 개발자들에게 적극 권고한다.

또한 모든 동적생성Web페지들에서 문자모임들을 해당한 값으로 명백히 정하여야 한다.

자료의 코드화와 려과가 이 취약성을 해결하는데서 중요한 단계이며 또 복잡한 문제이므로 CERT/CC는 이 문제를 보다 구체적으로 해석한 다음의 주소에 있는 문건을 볼것을 권고한다.

http://www.cert.org/tech_tips/malicious_code_mitigation.html

Web봉사기관리자들은 해당 판매업체에서 보강프로그람들을 구입하여 적용해야 한다.

일부 Web봉사기제품들에는 동적으로 생성되는 페지들이 기정설정값으로 들어 있다. 만일 당신의 싸이트에 자체로 개발한 동적페지들이 없다 하더라도 당신의 Web봉사기는 여전히 취약하다. 실례로 당신의 봉사기가 생성한 《404 Not Found》페지에는 악성태그가 붙어 있을수 있다.

이 문제를 해결하자면 Web봉사기관리자들은 자기의 해당 판매업체가 제기하는 보강프로그람들을 적용하여야 한다. 부록 1에는 이 정황보고서를 위하여 판매업체들이 제공하는 정보들이 들어 있다. 더 많은 정보를 받는 차제로 우리는 이 부록을 갱신할것이다. 목록에서 당신의 판매업체의 이름이 없으면 CERT/CC는 그 업체에서 정보를 받지 못한것으로 된다. 당신의 판매업체와 직접 련계를 가지라!

제２８장. 확고한 보안: 새로운 보안세계질서

켄 사우레트

자신과 다른 사람들의 경험으로부터 배우는 자가 현자이다.

우리의 미래는 과거와 현재 그리고 우리들의 지향의 반영이라고 말할수 있다. 과거는 우리에게 무엇을 지향하고 무엇을 해야 하며 무엇을 하지 말아야 하고 무엇을 아직 모르는가 하는데 대한 지식과 지혜를 준다. 점쾌나 볼줄 안다는 보안전문가들이 과연 미래를 단순히 과거의 갱신된 재현으로 보겠는가. 미래의 기술과 회사, 경쟁업체, 제공업체, 소비자들이 그 기술을 어떻게 리용할것인가를 예언한다는것은 거의 불가능하지만 오늘의 현실이 과거에 그려 보던것과 그렇게 현저하게 차이나지 않는다는것은 자명한 사실이다. 그러니 그것을 《예언》이라기 보다는 《계획》이라고 불러야 할것이다.

표 28－1　　　　　　기본제목들과 인용문들(과거)

1981. 4. 20	주간 상업:《콤퓨터범죄–상업활동에 위험 증대》
1985. 7. 7	텍싸스주 뉴싼안또니오표명:《콤퓨터강도들 은행습격》
1987. 2. 4	콤퓨터세계:《범죄를 축출하라. 자료는 전략적자원이므로 MIS는 이 귀중한 재산을 보호하는 방법을 알아야 한다.》
1989.3	은행업에서 콤퓨터:《통과암호방위는 승용차가 주차할 때 열쇠를 건사하는것과 마찬가지이다.》
1990.2.12	콤퓨터세계:《그리고 통과암호는 쓸모 없게 되였다. 기억된 콤퓨터통과암호가 시대에 뒤떨어 졌는가, 극히 일부분의 콤퓨터과학자들과 보안전문가들은 그렇다고 생각한다.》
1990.10.14	자치적인 영국 런던:《해커들 5개의 은행 략탈》
1992.12	망관리:《전문가들 망보안이 호전되고 있지 못하다고 혹평》

그것을 어떻게 부르든 상관없이 모든 분야의 전문가들은 무역잡지와 보안일지들에 미래의 정보보안을 예측하는 기사들을 싣는다. 표 28－1에 여러 무역잡지들의 주요제목과 인용문들을 실례로 주었다. 표 28－1의 주요제목들과 인용문들을 표 28－2에 준 최근 몇년전의것들과 대비해 보라. 별로 의의 있는것은 아니지만 미래에 대한 예언자적견지에서 보면 표 28－1의 8년전 혹은 그 이전의 기사들이 표 28－2의 최근 몇년전것들과 큰 차이가 없다는것을 알수 있다. 실례로 통과암호를 방어수단으로서 취급하는 《은행업에서 콤퓨터》의 1989년기사를 보라. 거기에서는 승용차의 관건문제가 아니라 바로 열쇠를 쥐는 문제에 대하여 언급하고 있다. 《개인용콤퓨터세계》의 2000년 6월호에서 전문가들은 통과암호시대가 끝나간다면 이라는 질문을 제기하고 있다. 이것이 10년정도 지나면

다음과 같은 주제의 기사를 보게 되리라는것은 의미하겠는가. 《모든 사람을 위한 콤퓨터잡지》2010년 최신기사, 《생체계측학, 스마트카드 그리고 지난해 원시적통과암호인증법을 종국적으로 청산한 두 요소인증법은 DNA 및 유전검사법의 가격인하에 의하여 사멸단계》

이 모든것이 확고한 보안세계의 건설과 무슨 관계가 있는가. 어리석은자만이 같은 실책을 반복하는 법이다. 과거에 대한 리해 다시 말하여 무엇을 하였으며 하지 못한것은 무엇인가 하는것을 연구조사한 기초우에서만 미래에 대한 정확한 표상을 공정하게 얻을수 있다. 많은 회사들이 메인프레임방식을 버렸지만 보안우려는 여전히 없어 지지 않고 있다. 사실 그 우려는 더 많은 곳으로 《확산》되였을 뿐이다.

표 28-2 기본제목들과 인용문들(현재)

1996. 9. 23	주간 Web: 《싸이버은행개척자들 보안투쟁, 재정적장벽》
2000.12.7	AP: 《세계적으로 싸이버범죄법결핍, 일부 나라들에서 법률을 갱신하기 위한 기초축성》
2000.6.29	개인용콤퓨터세계: 《통과암호의 시대는 바야흐로 끝나 가는가. 앞으로 통과암호와 PIN번호를 기억할 필요가 더는 없을것이다.》
2000.4.10	산업표준: 《공격 받는 상업, 싸이버항의단체들 반회사운동에서 공격과 속임수법 새로운 수준에 도달》
2000.12.11	APBnews.com: 《21살의 광신적인 배우희망자가 헐리우드명배우모집기관의 Web싸이트를 이른바 공격, 기밀예능시험목록을 절취하여 인터네트상에서 전매한것으로 하여 콤퓨터사기 및 절도죄로 기소》
2000.12.22	콤퓨터세계: 《…해커는 Egghead회사의 보안장벽을 부셔버린다. …해커는 회사가 신용카드번호들을 보관한 소비자자료기지가 들어 있는 콤퓨터체계에 가까스로 뚫고 들어 갔다.》

보안전문가에게 있어서 자료파괴(destruction), 자료로출(disclosure), 자료리용(use), 자료수정(modification)(DDUM)은 모두 매우 심각한 고려사항이다. 자료의 비밀성도 무결성, 리용성과 함께 여전히 문제이다. 역시 중요한것은 자료의 적시성과 타당성이다. Atomic Tangerine의 퇴역고문 Donn B. Parker는 자료의 복사본절취가 자료의 가치를 극히 떨어 뜨리지만 원본자료의 무결성에는 큰 영향을 미치지 못한다고 하였다. 실례로 현재까지 팔리지 않은 무역비밀절도를 들수 있다. 소유자는 원본무역비밀을 여전히 가지고 있지만 그 정보가 도난 당하여 공개되였으므로 그 자료는 더는 원래와 같은 가치를 가질수 없게 된다. 얼마나 많은 회사들이 생산자료의 복사본을 검사환경에서 아직 리용하고 있는가, 생산에서와 같은 보호가 그 검사환경에 제공되는가, 생산에 참가하였던 사람들만이 검사환경에서 그 자료에 접근할수 있는가. 자료의 원본복사본을 가지는것만으로는 불충분하다. 만일 회사의 수입산출자료와 같은 시간적으로 요긴한 자료가

도난 당하여 주식구입이나 보도매체에 리용된다면 비록 무효하다 해도 그 자료는 변하지 않고 그대로 있는것으로 간주될수 있다. 필자는 이것이 반드시 CIA구조를 무효화시키는것은 아니며 오히려 보강하는것이라고 주장한다. 그 자료가 도난 당하여 회사에 해를 주고 좋은 기회를 잃게 할수 있다는 사실은 자료보호의 가치를 증대시키는것으로 된다.

메인프레임시대로부터 상당히 안전하고 안정된 시대에 이르기까지는 20여년이 걸렸다. 의뢰기/봉사기방식이 나오고 일부 자료의 이동과 그의 처리가 사용자에게 더욱 접근하게 됨에 따라 그와 같은 우려와 새로운 취약점들이 다시 나타나게 되였다. 메인프레임시대를 공고히 한 그 20년간의 경험으로부터 배우지 않는다면 현존환경에서 그런 안정성을 수립하는데 또 20년이 걸릴것이다.

확고한 보안세계의 기틀형성

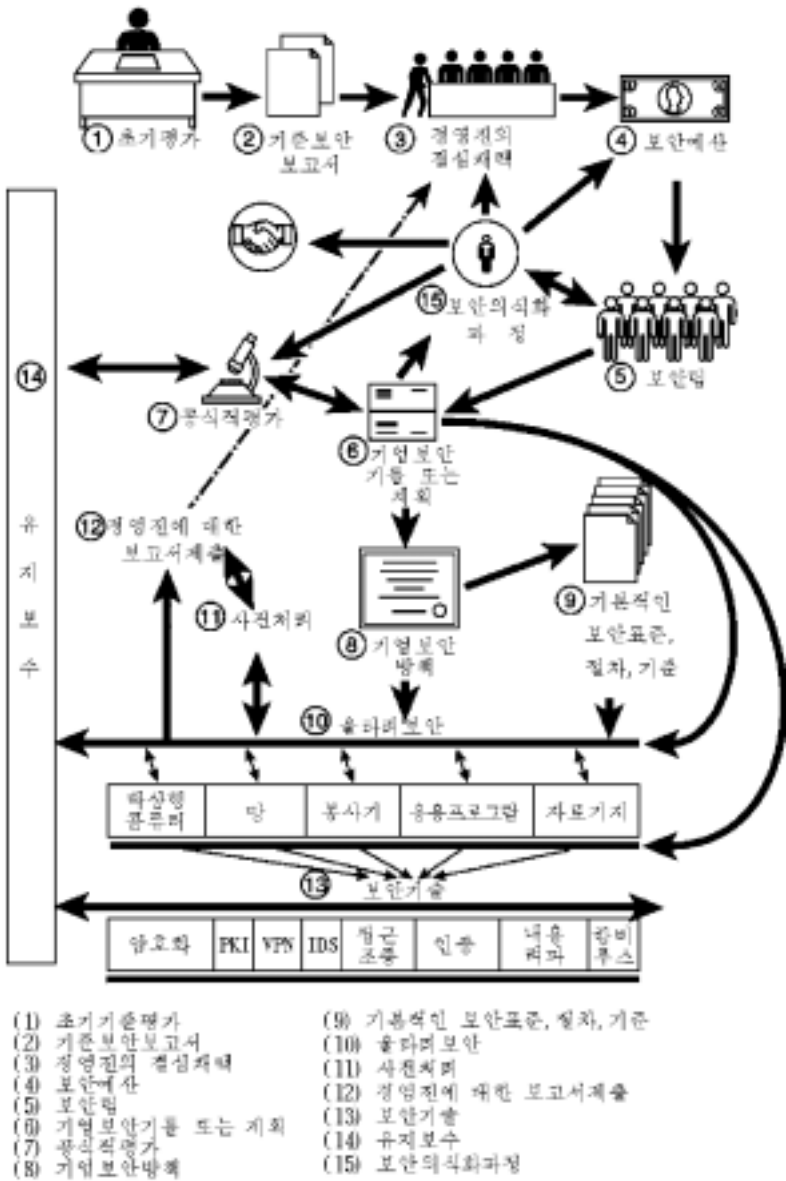
과거는 우리에게 어떤 교훈을 남기였는가, 과거에 대한 분석과 무엇을 하였고 하지 못한것은 무엇인가를 고찰함으로써 사람들은 미래의 보안구조들의 기틀을 형성해 나갈수 있다. 그 기틀은 업무공정의 자체평가가 완성될 때 형성되기 시작한다. 이것은 회사의 업무공정조사, 콤퓨터공정이 어떻게 그것의 효과성을 더 높이는가 그렇지 않은가, 새 기술이 어디에서 생산성을 증대시키고 새로운 수익을 주는가 등으로 구성된다. TCP/IP와 같은 새로운 규약들과 인터네트와 같은 기술들이 프레임중계(Frame Relay), 메인프레임(main frame), SNA(System Network Architecture)망과 같은 통신매체들을 대신하고 있기때문에 차이는 있지만 초보적으로 다음과 같은 네가지 측면에서 자료보호가 여전히 필요하다. (1) 발생측면, (2) 보관(주기억, 자료기지 혹은 디스크상의 파일, 여벌복사와 같이 오랜기간 보관하는 보관고에), (3) 처리(적용)측면, (4) 통과도중 또는 점 대 점 통신선로상에서 (망)

그림 28－1을 참고로 하여 다음의 문제들을 고찰해 보자. 그림에서 동그라미안에 든 수자들에 따라 론의를 진행한다. 업무공정과 통제를 비롯한 회사의 콤퓨터처리환경에 대한 첫 기준평가를 진행함으로써 회사는 자기의 보안세계를 옳게 구축할수 있는 비방으로 되는 구성요소들을 가지게 될것이다. 이 기준평가(1)을 실현하는 방법은 회사보안태세의 기준을 도출하기 위한 여러가지의 기초질문들을 제기(표 28－3 참고)하는것이다. 기초질문들을 완성하면 회사는 그 기초요구가 회사의 정보자산과 업무처리환경에 대한 모든 위험요소들과 로출점들을 충분히 반영하고 있는가를 곧 평가할수 있다. 이것은 조사결과를 문서화하고 업무처리환경과 로출점들을 최소화할수 있는 보안운영계획을 세울수 있도록 간명한 기준보안보고서(2)를 제출하는것으로써 달성될수 있다.

주의 초기기준평가는 보다 본격적인 《위험요소 또는 보안평가 및 분석》의 간략판이다. 자기 회사의 보안이 보기와는 달리 괜찮다고 오판되지 않도록 주의하라. 그 평가는 기초질문에 대답하는 사람들의 정직성과 지식 그리고 그 대답을 해석하는 사람들의 경험

과 지식에 따라 좌우된다. 실례로 회사가 자기 방책을 가지고 있다는 바로 그것으로 하여 꼭 그 방책대로 해야 한다든가 혹은 지어 그렇게 하도록 강요한다는것을 의미하지는 않는다. 사람들이 방책대로 하는가를 알아 보기 위하여 그 방책을 검사하면서 보다 세부화된 기준으로 평가할 필요가 있다.

그림 28－1. 확고한 보안세계

표 28－3 회사보안태세의 기준평가

1. 회사의 방책들이 명백하고 옳바른 전자우편사적비밀방책이나 인터네트리용방책과 같은것들을 준수하여 회사자원의 업무적리용문제를 취급하도록 정의되는가, 그것들이 시종일관하게 실시되는가 아니면 전혀 그렇지 않은가.
2. 회사의 조직체계가 알려 진 해킹취약점들의 로출을 방지하도록 가장 최신의 보안보강프로그람들로 갱신되는가, 회사의 체계에 접근하는데 어떤 취약점들이 악용될수 있는지 알고 있는가.
3. 회사는 콤퓨터범죄를 탐지할 능력이 있으며 경영진은 어떻게 그 범죄가 감행되고 누가 그 범죄의 범인인가를 법정과 보도매체, 주주들에게 립증할만한 명백한 근거를 가지고 있는가.
4. 회사는 가정 또는 무선으로부터의 원격접속을 허용하는가, 종업원들은 기관 사무실에서만 접속하는가, 어떤 방식으로 종업원들이 망에 접근하는가, 종업원들이 원격접근이나 탁상형콤퓨터상의 모뎀과 같은 경영진이 알지 못하는 어떤 방식들로 접근하지 않았는가.
5. 회사망을 통하여 무엇이 전송되는가, 극비 또는 기밀정보가 전송되지 않는가.
6. 정보처리보호대책이 PBX와 다른 전화회선을 통한 공격에 대한 보호에도 연장되는가.
7. 《우발적사건》에 대한 정의가 있는가, 우발적사건의 동기로 된 계획이 치명적사건을 초래하도록 작성되여 있지는 않는가, 경영진은 법정에 내세울만한 명확한 증거를 대면서 그 사건을 범죄로 기소할수 있는 능력을 키우려는 의향이 있는가.
8. 련방법률이 어떻게 기업활동에 적용되는지 관찰되였는가.
9. 모든 사용자들이 회사망을 사용할수 있도록 인증되고 권한이 있는가.
10. 회사의 모든 입구점들이 알려 지고 문서화되는가, 그것이 모뎀, 개인인터네트접속, 외부망접속 등과 같은 기술적문제로 하여 존재하는 문제들을 포함하는가.

보고서가 완성된후에 회사는 성공적인 보안계획작성의 첫째 문제 즉 경영진의 결심채택(3)문제를 취급하여야 한다. 기관마다 경영진의 결심채택기준을 매우 차이나게 정한다. 재정적손실을 일으키는 사건으로 하여 필요한 물건들을 벌충으로 사들이기 쉽다거나 경영진이 모든 위험요소들을 알고 있지 못하므로 그렇게 하기 어렵다라는 식으로 기준보고서에서 지적할수 있다. 업무구조에 그들을 인입시킴으로써 경영진의 리해를 도모할수 있다. 이 두 경우에 대처하여 경영진의 업무목적을 리해하고 보안우려에 대하여 경영진을 교육하는데 그림 28－1의 질문들을 리용할수 있다.

경영진이 보안문제를 최종적으로 결정하기전까지는 일반사용자들이 보안방책, 지침, 절차를 우선시하지 못할것이다. 보안문제가 심화되면 최고경영자로부터 인사관리자에 이르기까지 기관의 전반부서에 걸쳐 경영진의 려파시설을 설치하는것이 또한 중요하다.

보안은 보험처럼 일종의 희망을 안겨 준다는것을 명심하라. 보안은 보험과 같이 위험으로 인하여 가지게 되는 우려를 최소로 줄인다. 회사는 기업을 위험에 몰아 넣는 모든 취약점과 련관된 위험인자들에 대하여 수수방관할 의사가 전혀 없기때문에 돈을 들여서라도 보안대책을 강구한다. 보안은 회사가 자기의 보안이 경쟁자보다 우세하다는것을 보여 줄수 없는한 영업수익성을 증대시키지 못한다. 대부분의 회사들에서 보안은 수익을 내지 못한다.

보안은 업무비용에 속한다. 보안은 지출처럼 보이지만 업무의 필수비용으로 보아야 한다. 오늘 자료의존성으로 하여 회사가 보안계측을 할수 있겠는가 하는것이 문제인것이 아니라 그렇게 할수 없겠는가 하는것이 문제로 된다.

다음은 보안계획의 산물에 돌려 지는 예산(4)인데 그것은 경영진에 대한 지속적인 교육과 기술평가에 도움을 주며 보안기틀축성을 완성하는데 도움을 줄수 있는 보안전문가들이나 필요한 보안상담역들에 대한 적당한 로임을 포함한다. 예산은 또한 성공적인 사업을 도모해 나갈 팀에 제출되여야 한다. 그 팀(5)를 보안기틀 또는 계획(6)을 세우고 그것을 련속적인 결심채택과 잠정적인 추가예산요구를 위하여 경영진에 제출할것이다. 보안의식화과정(15)은 단순히 경영진에게 보안구조와 자금요구를 알려 주기 위하여 이 시점에서 진행되기 시작한다. 이 과정을 더욱 형식화하고 보안의식화과정초기의 리점을 살려나감으로써 경영진을 시종일관하게 자각시킬수 있다. 보안의식화과정은 그 과정이 형식화되는가 안되는가에 관계없이 보안과정전기간에 걸쳐 요구된다. 보안의식화과정에서는 경영진이 중요성을 인식하고 보안에 대한 지속적인 예산지원을 긍정하도록 그들에게 최근 사건들과 법률이나 규정들을 실례를 들어 알려줄 필요가 있다.

계획에는 확고한 보안세계를 세우기 위한 활동들을 우선시하는것을 포함시켜야 한다. 기관들에 따라 활동들을 우선시하고 지원체계를 수립(보안의식화과정을 통한 경영진의 결심채택)하도록 도와 주거나 기틀의 첨가 또는 변경을 확인하는데 공식적인 평가(7)를 리용할 필요가 있다. 평가를 실현하기 위한 초기 경영진의 결심채택과 예산은 여전히 요구된다. 기업전반적인 위험평가는 매우 많은 노력을 요구할수 있다. 평가에 기대와 목적을 두는것이 매우 중요하다. 이것은 특히 그 어떤 다른 평가도 진행된적이 없다면 매우 어려울수 있다.

평가는 회사전반과 그 처리환경을 포괄하는 공식적인 회사전반적평가로부터 선택된 환경에 대한 보다 작은 목적의 평가에 이르기까지 여러 형태가 있다. 실례로 침투시험이나 취약점탐색은 비합법적인 입구점의 로출을 찾아 내기 위한 회사의 외부접근에 대하여 실행될수 있다. 다른 하나의 실례로는 조작체계들의 상태와 그것들이 보안보강프로그람들을 놓치지 않았는지 또는 부정확하게 설정되였는지 하는것들을 결정하기 위하여 진행하는 호스트조작체계의 분석을 들수 있다.

공식적인 회사위험평가는 거의 틀림없이 보안과정의 수립이 계속되기전에 제일차로 요구될수 있다. 회사는 무엇이 필요하고 보안기틀에서 불완전한곳은 어디이며 우선시해야 할것은 무엇이고 방책에서 빠진것은 무엇이며 경영진에게 반드시 알려 주어야 할것은 무엇인가 하는것들을 어떻게 확인할수 있는가. 보안기틀의 매 요소와 그에 내포된 위험들이 다른 요소들에 영향을 미치며 매 위험은 완성된 기틀을 유지하는데 영향을 미치리라는것은 사실이다. 그러나 많은 회사들은 시간이나 돈, 대책들을 심중히 고려하여 기업전반의 위험평가를 진행하여야 한다. 특별한 목적을 가진 보다 작은 평가가 준수되면 첫째로 보안공정이 한층 강화될수 있다.

보다 작은 공식평가는 응용프로그람개발이나 봉사기, 망과 같은 기본보안구성요소들의 결함을 찾아 내는데 쓸수 있다. 이 단순한 평가는 응당한 주의를 돌려 수행하여야 할 기초적인 최선의 실천문제들을 확인하는데 도움을 줄수 있다. 이것은 보다 복잡한 공식적 또는 회사전반적인 평가를 먼저 요구하지 않고 시작할수 있도록 계획을 세

워 나갈수 있게 한다. 이런 경우 보다 공식적인 회사전반위험평가는 후날에 우선시될 수 있다.

법과 질서: 방책, 절차, 표준, 지침

모든 세계는 일정한 형태의 법과 질서를 요구한다. 회사보안방책(8)은 이 새로운 세계에 대한 골간과 방향이나 방도를 제공한다. 그것은 회사가 어디에 있으며 어디로 가려고 하는가를 정의한다. 이 보안방책은 업무공정에서 고수하여야 할 기준을 수립한다. 그 기준은 기관전반에 걸쳐 론리에 맞고 일관한 수준을 달성하기 위하여 자료처리환경의 매 구성요소(하드웨어, 쏘프트웨어)들에 대하여 규정된 보안통제수단이다. 지침은 일반기준 BS 7799(영국표준 7799)와 같은데서나 BS 7799이후의 국제적인 표준모형을 채용하기 위한 시도들(ISO 17799)에서 문서화된다.

방책과 절차는 기술이 발전하는데 따라 또는 업무요구가 변하는데 따라 끊임없이 변한다. 방책의 수준은 여러가지이다. 높은 수준의 방책은 상당히 포괄적이여야 하며 다음과 같은 항목들을 담고 있어야 한다. 《모든 콤퓨터체계들은 비루스검사도구들을 최신비루스부호들로 유지갱신하여야 한다.》이것은 경영진의 지도서이다. 보다 낮은 수준의 방책들은 회사가 표준화한 특정비루스검사쏘프트웨어를 문서화한 보다 기술적인 문서나 표준화안이다. 절차는 방책을 지원하는 단계적인 활동이며 비루스부호들을 유지갱신하거나 표준비루스도구들을 사용하는 방법에 대한 규정들을 확인할것이다. 이 낮은 수준의 방책들은 경영진과 회사에서 일관하게 집행되여야 할 결심채택을 안받침하면서 유지갱신하고 발전시켜 나가야 한다. 높은 수준의 방책은 보다 적게 변하지만 그래도 정기적으로 관찰되여야 하며 경영의 업무모델에 적용할수 있는가를 알기 위하여 지어 시험까지 해보아야 한다. 방책도 프로그람과 꼭같이 앞으로의 참조, 경영진의 조사, 실행인증(마지막 서명) 등을 위한 낡은 판번과 함께 판번조종을 하여야 한다. 이런것들은 기초적인 경영변경의 필수적인 구성요소들이다.

울타리보안

> 어리석은 자는 콤퓨터를 무시하지만 현명한 사람은 그것을 자기의 가장 맹렬한 도전대상으로 여긴다.

이 확고한 보안세계의 겉면은 매 가동환경에 맞는 기본 보안해결계층들로 덮여 있다(이 장에서 이야기하는 가동환경은 자료에로의 접근을 제공하는 어떤 처리환경을 의미한다). 이 계층들은 어느것을 택하는가에 따라 OSI참조모형의 7개계층 즉 물리층, 자료련결층, 망층, 전송층, 대화층, 표현층, 응용프로그람층들의 매 계층에 해당하는 보안계층이나 혹은 취약성계층이 될수 있다. OIS모형은 각이한 콤퓨터들을 인터패이스로 련결시킬수

있게 하는 규약계층들의 모임이다. 보안은 물리적이거나 기술적이거나 론리적인 그리고 관리적인 구성요소들과 밀접히 련관된다. 조작체계와 개개의 자료기지 그리고 각이한 망구성방식들의 차이나는 특징은 모두 자료처리를 위한 가동환경들을 제공한다. 그것들의 구조는 특수하고 매 가동환경마다 서로 다른 약점이 있으며 최대한의 보호를 위하여 특별한 설계와 설정 또는 제3자기술을 요구할수도 있다.

울타리유지보수(14)는 가장 도외시될수 있는 보안취약성의 하나이다. 울타리의 유지보수는 쏘프트웨어나 하드웨어가 최신으로 갱신되지 않거나 알려 진 보안보강프로그람들이 적용되지 않기때문에 자체로 그리고 저절로 진행되지 않는다. 일반적으로 공격자들은 자기들의 도구로 가동환경에 있는 알려 진 취약점들을 탐색한다. 취약성조사쏘프트웨어에 의하여 취약점이 발견되면 그것들을 수정하고 이 로출점들을 제거하기 위한 보수를 진행한다.

그림 28－1에서 (12)로 표시한 경영진에 대한 보고서제출에 따라 경영진은 제기된 의견을 접수하고 사건에 대한 정보를 유지보수하는데 필요한 예산요구로부터 제기되는 보안의 필요성을 분석한다. 이 단계의 보고서제출은 경영진의 결심채택을 안받침한다. 만일 경영진이 예산에서 약속된 돈이 어데로 나가는가에 대하여 전혀 귀를 기울이지 않는다면 필요할 때 추가예산지출을 더 줄일것이다. 이것은 전체 주기를 반복시킨다. 하드웨어, 최신쏘프트웨어제품판, 보안보강프로그람, 자료기지 또는 증강된 경로기와 다른 망기술들은 갱신될수 있다.

실속 없는 사람: 탁상형콤퓨터

탁상형콤퓨터는 여덟번째 취약성에 가장 가까우며 어떤 망에서도 흔히 가장 취약한 점 즉 《사람》으로 고찰된다. 놀랍게도 그것은 흔히 개선된 보안에 대한 맨 마지막 취약점으로 간주된다. 탁상형콤퓨터는 가장 많고 대체로 조종할수 없는 입구점을 의미하므로 그렇게 되기가 일쑤이다. 지난 몇해동안 더욱더 많은 보안기술과 제3자판매업체들의 해결책들은 탁상형콤퓨터에 접근하는 방향에서 나오게 되였다. 보안의식(15)은 사람의 취약성에 주의를 돌리는 보안공정의 기초적인 해결책이다.

인증, 권한부여, 구좌처리를 임의의 보안기술의 주요구성요소로서 간주하라. 권한부여는 탁상형콤퓨터를 사용하는 사람들에 대한 적당한 인증에 의거한다. 접근조종체계들 례컨대 생체측정, 스마트카드, 통표 지어 PKI같은것들은 모두 의뢰기 실행에 의존하며 흔히 탁상형콤퓨터에 접근하는 의뢰기대화에 의존한다. 실례로 다른 조종이 없는 PKI는 사용자의 인증을 제공하지 않지만 워크스테이션이나 무릎형콤퓨터를 인증하거나 열쇠가 권한 있는 사람의 손에 있는가 하는데 무관계하게 그 열쇠를 어떤 위치에든 보관한다. 실제의 인증루틴들은 봉사기에서 실행될수 있지만 필요한 통합을 실현하기 위하여 탁상형콤퓨터응용프로그람이나 조작체계와 련결하는데 흔히 의뢰기코드가 요구된다. 앞에서도 언급하였지만 흔히 탁상형콤퓨터가 너무 많기때문에 실현비용이 높으며 완전판과 성공적인 실현때문에 말단사용자로부터의 통합을 요구한다.

력사적으로 볼 때 많은 회사들에서 말단사용자가 보안을 개선하는데 도움을 주는 어떤 행동을 할것을 기대한다는것은 바람직할만한 일이 못되였다. 이것은 말단사용자들이 더 많은 콤퓨터상식을 알게 되고 기술이 보다 친절해 지면서 점차 호전되여 가고 있다. 이것은 또한 견실한 보안의식화과정(15)을 통하여 그들에게 방책, 표준, 절차들을 계속 알려 줄뿐아니라 기술과 가동환경의 알맞는 리용에 대한 부단한 교육을 줌으로써 개선되여 나갈수 있다.

간선도로와 측선도로: 망

도로는 사회들간의 련계를 지어 주는 수단이다. 망은 도로와 많은 측면에서 아주 류사하다. 자료처리세계에서 망은 사용자와 자료사이의 통신(련계)을 제공한다. 자료가 보관된 위치나 사용자의 물리적위치에 관계없이 망은 사용자의 접근을 보장할수 있다.

북부지방의 나라들에는 두개의 계절 즉 겨울철과 도로건설계절만이 있다고들 한다. 도로와 같이 망은 빈번한 감시와 정상상태를 보존하며 원활하고 안전하게 동작하도록 하기 위한 유지보수를 필요로 한다. 훌륭하게 건설된 도로가 안전한 수송을 보장하듯이 알맞게 구축되고 설정된 망은 안전하고 비밀이 담보된 자료의 전송을 보장한다. 그러나 원활하게 동작하는 망이 반드시 비밀이 보장된 망이라는것을 의미하지는 않는다. 일반적으로 망의 기능은 한곳에서 다른곳으로 비트렬의 전송을 보장하는것이다.

IDS(Intrusion Detect System), VPN(Virtual Private Network), 일반적인 망암호화와 같은 기술들(13)은 모두 망의 보안을 강화시킨다. IDS는 해당 직원에게 우발적인 사건에 대하여 경고하고 의심스러운 활동을 보고함으로써 망의 보안에 기여한다. VPN은 공공망 즉 인터네트를 리용하여 망들을 서로 안전하게 련결하도록 한다. 간단히 말하여 3DES나 IPSec와 같은 암호화규약을 리용하는 《가상턴넬》이 비밀전송을 보장하면서 망들사이에 설치된다는것이다. 만일 이것이 정확히 설정되면 파케트가로채기와 통과암호절취를 막을수 있다. 본질상 VPN은 비밀을 담보할수 없는 인터네트규약상의 두 점사이에 암호화를 리용하는 믿음직한 턴넬을 제공한다. 암호화통로를 통하여 자료는 보관고로부터 사용자에게 전송되는 선로상에서 위장된다.

도시, 구역 및 마을: 봉사기와 호스트

오늘 호스트나 봉사기들의 형태나 조작환경은 다양하다. 지난 시기에는 MVS, VM, DEC–VAX등의 메인프레임지향체계들이 있었다. 메인프레임은 봉사기와 탁상형콤퓨터의 모든 기능을 다 가질수 있었을뿐아니라 오늘날 여러 봉사기들에 보급된 지어 각이한 조작체계상에서 운영되는 그러한 봉사까지 각이한 《가동환경》들에 제공할수 있었다. 오늘날의 메인프레임(지금은 기업용봉사기로 더 잘 통한다)들과 일부 보다 강력한 봉사기들은 가동환경에 따라 가상적인 분산을 제공하지만 그것은 모두 같은 물리적인 《함》에

존재한다. 가동환경마다 자료기지봉사기, Web봉사기, 응용프로그람봉사기 지어 보안봉사기와 같은 그러한 전문봉사를 제공한다. 이 개개의 봉사기는 다른 조작체계를 가진 물리적으로 다른 하드웨어에 존재할수 있다. 이것은 명백히 보안조종을 위한것이 아니라 성능조종을 위한것이다.

호스트나 봉사기들은 기본적으로 다음과 같은 4개의 취약성계층을 가지고 있다.

1. 하드웨어(물리적함 실례로 특별한 설정을 할수 있는 내부구성요소들, 메모리, CPU)
2. 기본입출구(I/O: input/output)나 펌웨어. 이것은 CPU에 처리자료를 제공하거나 정보를 보관고나 인쇄장치로 보낸다.
3. 조작체계의 커널 또는 핵. 이것은 도시중심부의 아주 중요한 부분에 비유할수 있는데 바로 이 부분이 도시의 나머지 부분을 움직인다.
4. 조작체계인터네트 혹은 쉘. 실례로 사용자들에게 자기의 친절성을 보장하는 지령렬인터페이스나 그라픽스사용자인터페이스를 들수 있다.

물리적장치나 조작체계는 도시에서 건물과 비교할수 있다. 다양한 건물들은 구색에 맞게 봉사할수 있도록 자기의 구조를 가지고 있다. 은행은 금고실의 돈을 보호할수 있도록 특별히 견고하게 건설하지만 식당은 밖에서 차에 탄 고객들도 쉽게 식사를 요청할수 있도록 차에 탄채로 들여 다 볼수 있는 특별한 창문과 확성기체계를 구비한다. 특별한 조작체계를 가진 봉사기들은 방화벽에 의한 보호를 보장 받을수 있도록 견고하게 구축되는가 하면 공공자료를 지원하고 사용자들의 쉬운 접근이나 일반자료의 리용을 보장할수 있도록 열린구조로 구축될수 있다.

이러한 계층들을 서로 무난히 결합하여 적합한 콤퓨터보안가동환경을 구축하는것은 꽤 해볼만한 일이다. 보안체계는 물리적인 절도나 부정적행위로부터 내부구성요소들을 보호할수 있도록 고려되여야 한다. 경보장치들, 물리적인 관건장치들 또는 적합한 환경 및 접근조종장치들로 조종되는 콤퓨터실은 하드웨어를 보호할수 있도록 한다. 여러 제3자판매업체에서 제공하는 접근조종체계들을 구입하여 커널의 기본보안을 강화하거나 지령의 실행권한과 메뉴선택권한이 있는 사람들의 조종명부를 리용하여 주변장치들에 대한 접근조종을 할수 있다.

도시, 구역 및 마을의 운영: 응용프로그람

응용프로그람은 조작체계와 자료기지에 크게 의존하며 이러한 계층들을 가지고 원활하고 안전한 처리환경을 보장할수 있도록 설계된다. 조작체계(OS)와 통합하거나 자료기지(DB)에 밀접히 통합되는 응용프로그람은 적응성이 가장 좋으며 OS나 DB의 고유한 특징에 영향을 줄수 있다. 이것은 자기자체의 인증과 검사에 의존하는 응용프로그람을 대신할것이다. 통합된 응용프로그람은 부차적인 인증계층이나 업무처리의 복잡성이 없기때

문에 사용자가 모두 리용할수 있는것이다.

만일 응용프로그람이 자기자체의 인증에 의존한다면 그것은 필경 추가적인 약점을 로출시키며 말단사용자를 위한 또 하나의 루틴도 끌어 들일것이다. 어떤것은 보안을 위하여 또 하나의 통과암호와 추가적인 인증을 더 요구하지만 사용자는 어디까지나 취약한 통과암호를 선택하여 써넣기때문에 계속 더 다른 통과암호를 고안해 내도록 하는 사람의 속성은 쓸데 없는 시간랑비만을 추구할뿐이다. 조작체계가 이미 인증을 보장하지만 왜 그것을 믿지 않고 다시 인증하는것을 피하지 않는가.

응용프로그람이 보장하는 특별한 업무기능은 그 응용프로그람에 내장된 특별한 기능을 가진 응용프로그람준위의 보안을 요구한다. 이 기능들은 어느 사용자가 어떤 특수기능을 수행할수 있는가 하는것을 조종할수 있어야 한다. 사용자를 확인하기 위하여 특수한 인증을 응용프로그람자체에 제공하기보다는 오히려 그 응용프로그람이 사용자가 이미 조작체계준위에서 인증되였다는것을 믿도록 하는편이 낫다. 응용프로그람은 사용자가 수행할수 있는 기능들을 조종할수 있도록 자체의 인증구조를 가질수 있지만 그 인증을 진행하기 위하여 조작체계나 자료기지와 인터페이스로 련결되여야 한다. 이를 위한 한가지 방법이 응용프로그람이나 조작체계의 API(Application Programming Interface)들을 제공하는것이다. 이 API들은 응용프로그람과 조작체계사이의 통합 또는 스마트카드, 토큰, 공개암호열쇠, 생체측정 등의 제3자판매업체기술들과의 통합과 같은 주문화기능을 제공한다.

도서관과 학교: 자료기지

자료기지는 자료 또는 처리된 자료(정보)의 그릇이다. 그것은 대부분의 회사들이 보호하려고 하는 실체 즉 자료에 가장 가까운 대상이다. 자료기지는 보안정보, 응용프로그람조종, 메타자료 또는 자료에 대한 자료 그리고 단순히 기초자료자체 등을 담고 있을수 있다.

자료기지도 응용프로그람과 같이 사용자가 누구인가를 확인하기 위한 인증에 의거함으로써 사용자들이 접근할수 있는 대상과 적당한 련관을 맺도록 해준다. 인증은 그 다음에 자료요소들(테블, 렬, 마당, 행)에로의 사용자의 접근을 확인하는데 접근준위(갱신, 삽입, 삭제)는 물론 자료기지편의프로그람에로의 접근형태(반입, 반출, 신기, 부리우기, 압축)도 함께 확인한다. 응용프로그람보안이 철저히 실현된다 하여도 해당한 사용자들만 그 응용프로그람기능에 접근할수 있게 자료기지에서의 인증과 권한조종을 진행하지 않으면 자료에 직접 접근하도록 자료기지봉사가 제공된다. 이것은 감시자들에게 자주 발견되는 《뒤문》이나 취약점을 산생시킨다. 이 봉사들은 응용프로그람보안을 《우회》하며 그 응용프로그람에 내장되여 있을만한 어떠한 편집기능이나 조종기능을 가지지 않는다. 이때문에 자료를 질의하고 수정하려는 사람들은 그 응용프로그람을 리용하지 않으려 하며 다른 도구들을 써서 보다 직접적으로 그 자료에 접근할것이다. 대부분의 관계형자료기지관리체계(RDBMS)들은 자료를 직접 관리하기 위하여 SQL이나 기타 직접접근보고도

구와 같은 언어들을 사용할수 있도록 한다. 실례로 Peoplesoft 7.0응용프로그람체계는 인증과 권한부여 등을 포함하여 견고한 보안기능들을 내장하고 있지만 PeopleSoft구성방식이 의존하고 있는 RDBMS구좌들이 알맞게 설정되여 있지 않고 이 자료기지구좌들이 정확히 관리되지 않는다면 모든 PeopleSoft자료에로의 접근은 자료기지를 통하여 직접 와해될수 있다. 취약하게 설계된 Web응용프로그람을 또 다른 하나의 실례로 들수 있다. 응용프로그람은 자기의 임의의 사용자의 모든 접근에 대하여 단일한 포괄적인 자료기지구좌를 요구한다. 그 구좌는 자료기지에 접속하기 위하여 응용프로그람에 반영하기 힘든 고정된 통과암호를 설정할것을 요구한다. 하나의 구좌에 뚫고 들어 가면 전체 프로그람이 와해된다.

이 약점을 처리하기 위한 한가지 방도는 조작체계의 기능내에서 쉘들(UNIX)의 리용을 제한하여 하나의 구좌가 조작체계준위에서 수행할수 있는 기능을 조종하는것이다. 실례로 UNIX환경의 DB2UDB자료기지는 본 조작체계에 의거하여 인증(통과암호검사)을 진행하고 사용자구좌가 속한 그룹을 관리한다. 구좌는 실제로 조작체계에 접속하지 못한다. 구좌기정값 쉘에 빈 쉘을 할당하여 그 구좌가 그 준위에서 실제로 아무런 기능도 수행하지 못하도록 할수 있다. 이렇게 하면 어떤 UNIX쉘도 열리지 않고 조작체계와의 임의의 쎄션을 종결시키지만 통과암호검사는 여전히 발생되고 자료기지에로의 접속도 여전히 동작한다.

다른 하나의 인기 있는 RDBMS인 기초 ORACLE은 아주 취약한 고전적보안기능을 가진다. Braintree System(Pentasafe)SQLSECURE와 같은 제3자기술은 자료기지보안인증, 권한부여, 구좌감시특성들을 강화시킬수 있다. 이 도구들은 자료기지나 조작체계에 대한 접근조종체계들, 탁상형콤퓨터나 봉사기용항비루스도구들, 암호화(공개열쇠기반)나 가상개별망(VPN)들, 침해방지체계(IDS)들에 대하여 호스트기반이든 망기반이든 관계없이 모두 기초환경에 대한 보안수준을 강화하고 기본가동환경이 자기의 취약점을 개선할수 있게 하는 보안기술들(13)이다. 그러나 잘못 유지갱신되는(14) 기술들은 늘어 나는 복잡성뿐아니라 유치하게 유지되는 조작환경과 같은 새로운 취약점들을 초래한다.

보안주기: 요약

> 다른 사람들의 실수로부터 배우라. 남들이 범한 실수를 자신이 직접 체험하려면 일생을 살아도 모자랄것이다.

과거는 우리에게 무엇을 가르쳤는가. 사람은 과거의 실수들에서 배울 필요가 있다. 하드웨어나 쏘프트웨어에 대한 유지보수나 갱신을 하지 않으면 과거의 실수를 되풀이하

게 하는 비합법적인 접근과 같은 취약점들을 그대로 가지고 있게 된다. 알려 진 취약점들은 비합법적인 접근의 근본원인으로 되며 처리환경의 안정성을 위협한다.

많은 회사들은 자료처리에서 메인플레임방식으로부터 분산형체계방식으로 이동하였지만 보안조종은 그에 따라 서지 못하였다. 새로운 환경은 메인프레임방식에서 그러하였던것처럼 조종감시에 응당한 주의를 돌릴것을 요구한다. 낡은 환경에서 완전무결하였던 방법론들을 새로운 처리환경들을 구축하는데 리용함으로써 옳바른 환경구축에 드는 시간을 절약하라.

여덟개 계층의 취약성이 있다. 이 계층들은 물리적계층, 기술적계층, 관리자계층들로 꼭 맞아 떨어 진다. 세부취약점들은 OSI참조모형의 물리층, 자료련결층, 망층, 전송층, 대화층, 응용프로그람층들과 운영자이든 사용자이든 누구나 가장 큰 실수를 로출시킬수 있는 가장 곤난한 취약성조종계층으로 구분된다.

확고한 보안세계를 구축하는 사업은 업무처리모형을 구성하는 모든 계층들에 주의를 돌릴것을 요구한다. 매 층마다 고유한 취약점들을 드러 낸다. 완성된 해결대책은 기술문제에만 귀착되는것이 아니다. 관리, 경영, 처리는 모든 보안해결대책의 중요부분들이다. 보안공정전반에 대한 리해는 포괄적인 보안계획작성을 도모한다. 전반계획은 경영진의 결심채택과 충분한 예산 그리고 경영자를 교육하고 서로 의견을 나누며 경영자 혹은 경영진에 조사결과를 제출하여 모든것들을 서로 결합시키는 보안의식화과정이 있는 방책이라는 지침을 가짐으로써 보안흐름의 주기를 유지하도록 한다.

제29장. XML과 기타 메타자료언어에 대한 보안

윌리암 하흐 말레이

필자는 어린 나이에 착공카드장치조작공으로 일하였다. 이 기계는 원시적인 정보처리기였으며 여기서 정보는 종이에 뚫린 구멍형식으로 기억되였다. 이전의 관점에서 보면 종이는 상대적으로 보잘것 없지만 현대적관점에서 보면 대단히 가치 있는 자료의 보관고이다. 례를 들어 1Gbyte의 기억은 착공종이로 환산하면 보통 크기의 방을 공간 없이 꽉 채울 정도였다. 종이는 자료의 보관고로서 가치가 있었지만 기록량에 있어서는 엄연한 한계가 있었다. 《단위기록》은 홀러리스코드(Hollerith code: 80×12착공카드에 자료를 표현하기 위한 코드–역주)로 쓸 때 80개 문자로 한정된다. 이 코드는 평균 초당 10~15개 문자를 읽을수 있다. 병렬로는 분당 8~12K를 읽는다.

그러므로 응용프로그람설계자들은 흔히 고밀도부호화를 쓴다. 례컨대 날자로서의 년도는 흔히 한개 수자로 또는 응용프로그람에 따라 두개 수자로 기억되였다. 이것이 유명한 2000년문제의 시원이였다. 2000년문제가 해결되였으므로 이 문제를 흔히 프로그람작성의 론리적문제로 생각하였다. 즉 프로그람은 기억된 년도를 4개의 수자로 처리하지 않으므로 2000을 1999의 다음이 아니라 이전으로 해석한다. 이것은 또한 자료의 질문제와 관련되기도 하였다. 년도를 1개 또는 2개의 수자로 코드화할 때 흔히 정보는 완전히 상실되였다. 문제를 확정하자면 자료가 무엇인가 하는것을 추측해야 하였다.

착공카드기록에서 문자의 의미는 그것이 놓인 위치에 의하여 결정된다. 례컨대 구좌번호는 카드의 1렬부터 8렬사이에 기록되여야 한다. 안정한 대규모응용프로그람의 착공카드장치조작공들은 흔히 카드에 구멍 뚫린것을 보고 그 응용프로그람의 기록을 알수 있으며 마당을 구획지어 갈라 볼수 있게 된 카드표면을 보고 어떤 정보가 어느 렬에 기억되여 있는가 하는것을 결정한다.

파일의 이름은 흔히 카드에 구멍을 뚫어 부호화하였으며 마당의 이름은 카드에 있는 그 위치로 부호화하였다. 부호표는 코드앞면에서 인쇄되든가 또는 따로 기억되였다. 어느 경우이건 조작공은 그것을 리해할수 있었지만 기계는 그렇지 못하였다. 즉 자료에 대한 자료는 기계가 리해할수 없었으므로 기계에 리용될수 없었다.

정보의미의 이러한 의미부호화와 종이에 갈라서 부호화하는 분산기록은 일찌기 콤퓨터프로그람작성에 도입되여 리용되였다. 그러므로 2000년문제해결에 착수함에 있어서 어디서 문제성들이 나타날수 있겠는가를 알아 내는데서 기계에 의거할수 없었고 프로그람과 자료밖의 원천을 참고하지 않으면 안되였다.

메타자료

현대식으로 말하면 자료에 대한 자료를 메타자료라고 한다. 메타자료를 리용하여 다른 방법으로는 서로 알수 없는 프로그람들사이의 자료통신을 보장한다. 자료기지스키마,

스타일쉬트(style sheet), 태그언어 그리고 지어 COBOL의 자료정의부분도 다 메타자료의 실례들이다. 지금은 기억이 빠르고 렴가이므로 현대실천에서는 자료가 서술되는 자료를 가진 메타자료의 보관을 요구한다. 많은 응용프로그람과 규약에서 메타자료는 자료와 함께 전송된다. 전자자료교환(EDI)이 좋은 실례로 된다. 여기서 마당들은 자료들의 의미와 그 용도를 태그로 전송한다.

고급한 사용자들은 메타자료형식으로 자료를 기억시키며 움직인다. 중요한 보안실천에 의하면 메타자료는 자료기지에서처럼 자료에 철저히 결합되여 예견하지 않은 변화를 방지해야 하며 그 어떤 변화도 명백히 하여야 한다. 객체지향콤퓨터환경에서는 자료와 그 의미 그리고 그 자료에 따라 수행할수 있는 모든 연산들이 단일객체로 묶어 질수 있다. 이 객체는 임의의 변화와 오해를 다 방지한다.

태그언어

태그언어는 메타자료의 한 형식이다. 태그는 특별히 형성된 마당으로서 자료에 대한 정보를 담고 있다. 태그는 위치로 나타낸 자료와 결합된다. 즉 태그는 자료에 선행한다. 태그는 임의로 그러나 종종 그 뒤와 해당한 끝태그의 앞에 있는 모든것에 관계된다.

XML은 태그언어이다. 이런 의미에서 HTML, EDL, GML과 비슷하다. 태그는 그와 내용적으로 련관된 자료에 대한 정보를 담고 있는 변수이다. 태그는 메타자료이다. 제한된 정도에서 태그들은 단어를 보존한다. 제한된 보존만이 요구되는것은 다른 태그언어에서와 같이 태그가 그 어떤 약속에 의하여 다른 자료와 구별되기때문이다. 례컨대 태그들은 그 왼쪽과 오른쪽에 거듭 인용부호들을 주어 <태그이름>과 같이 표시하든가 또는 :태그이름과 같이 두점으로 시작하여 태그이름을 쓰는 방법으로 표시한다. 이런 식으로 태그들을 구별할수 있다. 매개 태그는 우의 경우와 비슷하게 서로 구별되면서도 그와 련관된 끝태그를 가지고 있다. 례컨대 왼쪽에 거듭인용부호를 주고 빗선을 준 다음에 태그이름을 주는 식으로 즉 </태그이름>과 같이 또는 처음에는 두 점을, 그 다음에는 문자 《e》를 주고 그 오른쪽옆에 태그이름을 주는 식으로 즉 :e태그이름과 같이 끝태그를 시작함으로써 끝태그들을 구별할수 있다. 끝태그들을 리용하는것은 자료의 길이속성을 필요로 하지 않도록 하기 위한것이다. 태그들은 겹쳐서 사용된다. 례컨대 이름과 주소에 대한 여러개의 태그들이 이름과 주소에 대한 한개의 태그안에 나타날수 있다.

태그언어는 태그정의들의 모임이다. 모임, 언어, 언어변종 또는 스키마와 같은것은 문서형정의객체에서 정의된다. 이 스키마는 그것이 서술하는 객체안에서 교갑화되거나 또는 참조, 문맥 혹은 기정값에 의하여 그 객체와 련관될수 있다. 이 언어정의들은 겹쳐서 쓰일수 있으며 흔히 겹쳐서 쓰인다. 이것은 최대한의 기능과 유연성을 보장하지만 혼동을 일으킬수 있다.

《표식달기》의 개념은 편집과 출판으로부터 나온것이다. 필자는 문서를 편집자에게 넘겨 준다. 편집자는 필자와 인쇄공 또는 식자공과 련계를 위하여 본문에 《표식달기》를 한다. 초기의 태그언어는 일반표식언어(GML)였다. 이 언어가 아마 표식달기언어의 원

형인것 같다. 그러나 표식달기의 개념은 개개의 단계에서 수행되는것을 제시하여 원본에 값 또는 정보를 보충하게 한다. 표식달기언어라고 부르는 많은 태그언어들은 사실상 그 특별한 의미에서는 표식달기언어가 아니다.

대부분의 언어와 같이 태그언어들도 특수용도에 쓰인다. 태그언어에서는 특정한 문맥에서만 뜻을 가질수 있는 특수한 어휘들만이 쓰인다.

례컨대 재정봉사에서 단어 《보안》의 의미는 정보기술에서와는 다른 의미로 쓰인다. 이와 마찬가지로 EDI에서는 오직 자기들의 응용프로그람에서만 쓰일수 있는 X12, EDFACT, TRADACOMS를 비롯한 많은 각이한 어휘들이 쓰인다.

확장표식언어(XML)

XML은 자료요소들을 서술하는 언어이다. XML은 자료의 속성들을 서술하고 있으며 자료의 의미와 그 용도를 식별한다. XML은 매개 자료들과 련관된 태그들의 모임과 그 태그들을 해신하는 서술문들로 이루어 져 있다. 자료기지스키마와 기록의 설계를 생각해 보라. 이러한 언어들의 제한성들에 대해서도 생각해 보라. 그리고 XML을 HTML과 비교하여 생각해 보라. HTML이 자기 문서들의 연시 및 인쇄방법을 제시한다면 XML은 이런것들을 자기의 속성으로 가지며 바로 이것이 XML의 의미이다. XML은 마술사가 아니다.

XML은 열린언어이다. 때문에 이 언어를 확장할수 있는것이라고 한다. 물론 프로그람작성언어들은 어느정도 확장할수 있는것이다. 동적HTML은 10년전에 나온 HTML과 류사할 따름이다. 오늘의 열람기는 플라그인과 DOM(동적객체모형)을 리용하여 동적으로 확장될수 있다. 현대HTML은 동적으로 확장할수 있다. 해석능력은 플라그인과 애플리트 등을 리용하여 동적으로 확장된다.

XML을 리용하는 객체의 소유자는 자기가 선택한 임의의 태그들을 정의할수 있으며 그 정의를 객체에 내포시킬수 있다. 새 태그의 의미와 속성은 낡은 태그에서 서술된다. XML은 IBM에서 개발하고 ISO표준으로 채택된 표준일반표식언어(SGML: Standard Generalized Markup Language)의 변종이다. XML은 cXML(Commerce XML), VXML(Voice XML) 그리고 MSXML(Microsoft XML)까지 포함한 많은 변종의 원형이다. 산업용, 응용프로그람용 지어는 봉사용변종들도 있을수 있다. 그러나 임의의 변종언어의 가치는 그것을 사용하는 몇몇 대방들의 기능에 달려 있다.

XML은 세계적규모에서 쓰이는 언어이다. 말하자면 그것은 기업체들, 산업들 지어는 나라들의 경계를 넘어서 쓰이는 세계적스키마이다. 이 스키마들은 자료의 의미와 리용에 대한 사용자와 응용프로그람사이의 폭 넓은 사전약속을 표현하고 있다. XML의 어휘규모는 COBOL과 같은 프로그람작성언어의 규모와 대조된다. COBOL에서는 자료서술이 흔히 한 기업소범위내에 그리고 종종 단일프로그람범위내에 국한되여 있다. 여기서 동사의 기초모임은 기업소들사이에 공통적이지만 공통적인 명사들은 없다.

XML은 이름공간의 개념을 실현한다. 즉 XML은 이름과 그 의미사이에 하나이상의 약속을 제공한다. 목적하는 이름공간은 태그이름 앞에 있는 두점 다음의 공간의 이름에

의하여 지적된다(<ns:tagname>). 제한된 문맥에서만 쓰이는 많은 특수어휘들과 함께 비교적 작은 어휘들도 많이 약속할수 있다.

XML은 서술언어이다. XML은 서술문들을 명시적으로 생성한다. 이 서술문들은 절차에 관한것이 아니라 해석에 관한것이다. 그 서술문들은 어떻게 할것인가 하는것보다도 오히려 무엇인가를 나타낸다. 그러나 태그이름들이 임의의 절차의 등가물인 임의의 정의를 교갑화할수 있다는것을 명심해야 한다.

XML은 해석언어이다. BASIC, Java 및 HTML과 같이 XML은 응용프로그람에 의하여 해석된다. 그러나 일관성을 보장하고 XML의식응용프로그람을 쉽게 구축하기 위하여 대체로 표준적인 구문해석프로그람과 표준정의 혹은 스키마를 리용하게 된다.

XML은 재귀적이다. XML을 정의하는 객체인 XML스키마는 XML로 작성된다. 이 스키마에는 참조형정의들이 있다. 실례로 이 스키마는 보편적인 URL로 정의를 참조할수 있다. 사실 이런 리용방법은 태그에 대한 목적하는 정의를 찾는 가능성을 높여 주기때문에 일반적일뿐아니라 종종 권고되는것이다. 물론 자료소유자의 견지에서는 이런 리용법은 안전하다. 이 리용법은 소유자가 목적하는 정의들을 리용하여 태그들을 해석할수 있다는것을 소유자에게 담보한다. 자료수신자의 견지에서 보면 걱정스러운것은 오직 또 하나의 기만준위(즉 속임수)일수 있다. 여기서 좋은것은 URL들이 령역이름으로 시작되는것이다(한 령역의 이름들이 아주 믿음직하면서도 또한 위조된것들일수 있다). 메타자료의 의미가 개별적인 객체에 기억될수 있으며 또 흔히 기억되지만 국부정의는 대역정의를 무시할수 있다.

그 객체는 《형을 지적한》자료 즉 연산들의 특정한 모임만이 타당하게 되는 자료형태들을 지원한다. 그러나 XML로 정의된 자료의 모든 속성과 마찬가지로 자료에 대한 자의적인 연산들을 방지하는것은 언어자체인것이 아니라 언어의 응용인것이다. 실례로

```
<simpleType name=“nameType”>
<restriction base=“string”>
<maxLength value=“32”/>
</restriction>
</simpleType>
```

은“nameType”의 최대길이가 32로 되게 한다. 이런 류사한 메타자료는 다른 제한조건을 가하거나 문자모임, 대소문자, 유효값들의 모임 또는 범위, 소수의 자리 또는 임의의 기타 속성이나 제한과 같은 속성들을 정의할수 있다.

XML과 다른 태그메타자료언어들은 자료들에 크게 속박되지는 않는다. 말하자면 자료를 변경시킬 권한을 가진 사람은 메타자료를 변경시킬수 있다. 태그를 변경시킬 권한을 가진 사람은 자료로부터 그것을 분리시킬수 있다. 이런 유연한 결합은 메타자료를 변경시키는 경우에 자료자체를 변경시키는것과는 다른 특권의 모임이 요구되는 자료기지와 대조될수 있다(표 29－1을 볼것).

통신에 메타자료를 리용하는 좋은 실례는 전자지갑응용프로그람이다. 그 소유자는 전자지갑을 리용하여 전자인증서들을 기억시키고 사용한다. 이런 인증서들에는 이름과 주소, 사용자 ID들과 통과암호, 신용카드번호 등과 같은것들이 기록되여 있다. 이 모든 정보들은 로출되지 말아야 하므로 그것들을 흔히 자료기지에 기억시킨다. 자료기지는 자료를 숨겨 둘수 있고 그 자료를 메타자료, 예견된 의미 및 용도와 결합시킬수 있다. 반대로 메타자료와 파일암호화에 대한 태그들을 리용하여 단층파일에 자료를 기억시켜 리용되지 않을 때 기억장치에 그 자료를 숨겨 두게 할수 있다.

사용자는 전자지갑응용프로그람을 리용하여 여러가지 방법으로 인증서들을 제출한다. 례를 들어 사용자가 직결판매자로부터 구매할것을 결심했다고 생각해 보자. 선택을 한 다음 사용자는 화면의 검사단추를 누른다. 그러면 검사화면이 제시된다. 이 화면은 이름과 료금청구주소, 이름과 수화물주소 그리고 화물정보를 요구한다. 사용자는 전자지갑응용프로그람을 인입하여 이 화면을 완성한다.

전자지갑이 거기에 기억되여 있는 자료를 제시하면 사용자는 그것을 누르고 검사화면의 적당한 마당들에 끌어다 놓는다. 마당들에 표식들이 되여 있기때문에 사용자는 어떤 정보를 어디에 넣어야 하는가를 안다. 이 표식들은 HTML로 화면에 새긴다. 그것들이 사용자에게는 보이지만 전자지갑응용프로그람에서는 보이지 않는다. 그러므로 사용자는 전자지갑의 마당과 검사화면의 마당사이에 대응을 시켜야 한다. 이 과정이 유연하지만 여기서도 역시 시간이 걸리게 된다. 이 과정이 종국적으로는 바라는 결과를 얻게 하지만 여기서 자체정정귀환조종과 중간오유시정을 진행하게 된다. 사용자는 화면이 완성되여 만족하게 되면 Submit단추를 누른다. 바로 이때 화면은 판매자에게 귀환되며 판매자의 콤퓨터가 그것을 더 검증하고 또 한차례의 오유시정과정을 시작할수 있다.

화면의 마당을 HTML로 표식하는것외에 또한 판매자가 XML로 그 마당을 표식하면 XML을 아는 전자지갑은 사용자를 위한 검사화면의 부분을 자동적으로 판정할수 있다. 검사화면이 료금청구정보를 요구하는 경우에 전자지갑은 료금청구서를 완성할 정보를 그 전자지갑에 가지고 있는가 하는것을 살펴 본다. 여러가지 정보가운데서 하나를 선택해야 하는 경우에는 사용자가 선택하도록 한다. 화면이 사용자가 요구하는대로 완성되였으면 사용자는 Submit단추를 누른다. 화면이 판매자에게 귀환되면 자료는 판매자의 XML로 알맞게 표식되며 판매자의 XML을 아는 응용프로그람과 그의 기업상대자(즉 그의 신용카드거래봉사자)는 자료를 확인할수 있다.

XML을 리용할 때 사용자가 쓰는 응용프로그람 또는 그 형식은 변화되지 않았다. XML은 응용프로그람의 자료와 그 의미를 변화시키지 않았다. XML은 그것을 아는 응용프로그람들사이의 통신을 촉진시켰을 따름이다. XML은 응용프로그람들사이의 통신을 더욱 자동화되게 하였다. 자료는 예견한 곳에 기억되고 예견한대로 조종되며 예견한대로 통신에서 쓰인다. 응용프로그람은 더 자동적으로 동작하고 오유의 기회는 감소된다. 가장 유명한 Amazon.com과 일부 판매업체들의 응용프로그람들이 그런 수준의 자동화를 이룩하였다는것을 알아 두라. 그러나 그들은 자료를 재현하고 잘못된 곳에 기억시키는 피해를 보면서까지 자동화를 실현하고 있다. 즉 사용자자료가 판매자체계에 기억된다. 이것은 그런 자료의 타개를 초래할수 있으며 또 이미 그런 타개를 빚어 내였다. 자료가 고객의 의뢰기에서보다 판매자의 봉사기에서 더 잘 보호된다고 주장할수도 있겠지만 각이한 사용자들을 통하여 자료를 수집하는것도 또한 더욱 매력 있는 목표이다.

바로 각이한 열람기들이 있는것처럼 각이한 전자지갑응용프로그람들이 있게 될것이다. 사람들은 열람기가 HTML을 인식할것을 요구하며 마찬가지로 전자지갑이 판매자의 응용프로그람과 같은 XML의 변종을 인식할것을 요구한다. 전자지갑은 판매자의 응용프로그람과 같은 XML의 변종을 인식한다는것을 확인하기 위하여 열람기응용프로그람들이 여러가지 암호화알고리듬을 인식하는 방법과 류사하게 여러가지 XML변종들을 인식할수도 있다.

판매자의 응용프로그람이 사용자의 전자지갑으로부터 화면에 현시되지도 않으며 사용자가 제공하려고도 하지 않는 정보를 요구할수도 있다는것을 알아 두라. 사용자는 자기의 응용프로그람 즉 전자지갑의 거동에 의거하여 그것이 허용하는것만을 송신한다.

판매자의 응용프로그람이 전자지갑 혹은 그 자료들을 탐색하려고 할수 있는것과 같이 사용자는 판매자를 속이기 위하여 판매자가 보내는 태그들을 변경시키려고 할수 있다. 판매자는 자기의 응용프로그람에 의거하여 이러한 기만으로부터 자기를 보호한다.

XML의 능력과 제한성

모든 도구는 그것이 할수 있는 가능성과 제한성을 가진다. 제한성들은 바로 그 도구의 개념에 고유한것일수 있거나(즉 나사돌리개는 못을 박는데는 쓸모 없다) 실행과정에 생길수 있다(즉 나사돌리개의 손잡이와 날은 쓰는 과정에 류동이 있을수 있다). 도구는 그것이 적용되는 객체에 적합하지 않을수도 있다(즉 나사돌리개가 너무 크거나 너무 작으므로 나사를 돌릴수 없다). 파리잡이에 곽사포를 사용하지는 않는다. 이 절에서는 XML의 능력, 용도, 오용, 람용 및 제한성과 류사한 메타자료언어들을 취급한다.

XML은 메타자료이다. 그것은 자료에 대한 자료이다. 그 역할은 자료기지에서 스키마의 역할과 류사하다. XML의 기본역할은 자료의 일치성, 의미, 용도를 전달하는것이다. XML은 보안도구도 아니며 본질적취약성도 아니다. 보안의 관점에서 보면 그 고유한 역할은 통신을 지원하고 오유를 줄이는것이다. XML의 잠재적인 부적합성 또는 위협의 측면은 여기에만 유일하게 있는것이 아니다. 이런 측면은 다른 언어들, 메타자료, 태그들 등이 다 가지고 있는 측면이다. 흔히 진실을 전달하는데 쓰이는 언어도 거짓에 람용될수 있다.

사람들은 HTML을 리용하면서 HTML과 함께 거의 10년간이나 살아 왔다. XML이 XML에서 정의되는것처럼 XHTML이라고 하는 HTML 4.0판도 그렇게 정의된다(재귀개념은 흔히 혼란을 가져 오며 때로는 공포를 주기도 한다). 사람들은 거의 한 세대나 EDI태그들을 사용하여 왔다. 그 태그들이 지금은 XML의 부분모임이지만 그것들에 대한 모든 경험은 아직도 쓸모 있다.

아마도 XML에서 대부분의 보안우려의 근원으로 되는것은 XML이 《넣기(push)》기술과 함께 쓰이는것이다. 즉 자료를 서술하는 태그들은 자료와 함께 쓰인다. 더우기 자료해석스키마는 자료들에 포함될수 있다. 이 모든것은 수신자나 사용자에게 아주 많은 지식이나 목적이 없는 상태에서 일어 난다. 그러나 그 의미는 접수하는 체계에서 해석될것이다. 이것은 우려를 자아내지만 그 의미는 자기의 규정대로 해석된다. 자료의 송신자만이 예견된 의미를 아는것이다.

XML에서 보안에 대한 기본책임은 해석기에 있다. 열람기가 HTML로부터 파일체계

를 숨기는것처럼 응용프로그람은 XML로부터 그 파일체계를 숨겨야 한다. HTML태그를 어떻게 나타낼것인가 하는것은 열람기가 결정하는것처럼 XML태그의 의미는 응용프로그람이 결정한다. 그러나 이렇게 하는데서 응용프로그람은 호출한 구문해석자에 의거하여 그것이 태그들을 처리하게 도와 줄수도 있다. 응용프로그람이 구문해석자에 의존하는 한에 있어서는 그 응용프로그람이 쓰고 있는 구문해석자가 정확한것 이라는것이 확인되여야 한다. 일반적인 실천은 프로그람이 환경에 의거하여 호출한 프로그람의 신원을 보증하게 하지만 훌륭한 보안실천은 응용프로그람이 구문의 신원 지어 그의 수자식서명을 검사할 정도까지 확인할것을 요구할수 있다.

많은 해석언어들과 마찬가지로 XML은 그것이 해석될수 있으리라고 사용자 혹은 수신자가 기대하는 환경 또는 문맥에 XML이 지령을 보내도록 허락하는 도피기구를 호출할수 있다. 이것은 XML에서의 가장 심각한 로출일수 있다. 그러나 그것은 XML에서만 있게 되는것이 아니다. 거의 모든 프로그람작성 및 자료서술언어들은 그런 도피기구를 포함하고 있다. 이 도피기구들은 사용자가 자료라고 생각하는것을 처리에로 넘길 가능성을 가진다(표 29－2).

표 29－2 　　　　　　　　　　　　　Web우편 : 실례

《 Web우편 》은 보통의 2층(two–tier)의뢰기/봉사기전자우편을 3층(three–tier)의뢰기/봉사기프로그람으로 전환시킨다. 아마도 가장 잘 알려 진 실례는 Microsoft회사의 Hot–mail일것이다. 그러나 Excite와 Yahoo와 같은 다른 안내싸이트(portal site)들은 자기의 실행방법들을 가진다. 많은 인터네트봉사제공업체들은 자기의 우편사용자들이 임의의 기계로부터, 방화벽(HTTP는 허용하지만 우편을 제한하는)뒤로부터, 공공봉사기들로부터 그들의 우편국에 접근하도록 허락하는 실행방법을 가진다.

Web우편에서 통보문은 중간층(middle tier)에서 실제로 해신되고 다루어 진다. 그 다음에 통보문은 Web열람기에 의하여 워크스테이션에서 사용자에게 연시된다. 어떤 실현방법에서는 중간층이 태그들을 알아 볼수 없었고 Web열람기에로 태그들을 단순히 넘겨 주기만 하였다. 공격자는 이 능력을 리용하여 열람기가 사용자이름과 통과암호칸이 있는 Web우편접속창문을 연시하게 하였다. 경험 있는 사용자는 기대하지 않던 접속창문이 나올 때에는 응답하지 않았지만 경험 없는 사용자는 응답하였다. 모든 응용프로그람들이 예정한대로 동작할 때 공격자들은 그 프로그람들을 리용하여 사용자를 속일수 있었다. Web우편은 태그들이 단순한 본문방식의 안전한 우편환경으로부터 불안전한 열람기환경에로 들어 가게 하였다.

이 수법은 XML과 같은 언어들의 중요한 특징을 보여 준다. 이 특징은 언어들에 대하여 론할 때 흔히 스쳐 버리기 쉬운것이다. 이 언어들은 말단사용자에게는 투명하다. 말단사용자는 이 언어들이 전달하는 통신내용은 고사하고 이 언어들이 존재한다는것조차 알지 못하며 또한 자기체계, 자기응용프로그람 또는 자기 자신에게 의미가 어떻게 전달되는지도 모르는것이다.

그런 기구들은 대부분이 사용되기 시작한데 불과하지만 나쁘게 쓰일수 있는 잠재력을 가지고 있다. 비루스들은 Word, Excel 및 Visual Basic에 포함되여 있는 도피기구들을

교묘하게 리용하여 자신들을 실행하고 기억장치에 접근하여 복사본을 기억시키며 또한 사용자에게 오도된 정보를 연시한다.

Web보안

XML이 Web보다도 다른 많은 응용프로그람들에서 리용되지만 Web은 흥미 있고 중요한 프로그람이다. 론의된바와 같이 XML은 Web의 보안을 거의나 악화시키지 않는다. XML이 사용자들과 응용프로그람들을 속이기 위하여 사용될수 있는것은 사실이다. 그러나 그런 취약성들은 다른 언어 또는 방법들에 의해서도 역시 쉽게 람용될수 있다. 자료의 용도와 의미를 더욱 명백하게 함으로써 XML은 그 리해를 촉진시킬수 있다.

다른 한편 XML은 통신을 개선하고 오유를 줄이는 잠재력을 가지고 있다. XML은 Web의뢰기와 봉사기들의 능력을 확장하는데 쓰이며 그 응용프로그람들의 보안을 높여준다. 이 능력들은 다른 방법들로 실현될수도 있고 XML에 의해서도 실현된다. 이 능력이 메타자료언어로 실현되고 있다는 사실은 그런 언어들의 한가지 우점을 보여 주는것이다. 이 실현들은 가동환경과 전송에 대하여 다 같이 독립적인 운용호환성을 포함하여 메타자료언어들의 많은 우점들을 보안할수 있는 잠재력을 가진다. 그러나 이런 정의들은 XML의 보안에 관한것이 아니라 오히려 보안을 위한 XML의 리용에 관한것이다.

XML객체에 대한 접근조종

그런 한가지 응용방법은 Web봉사기들에 보관된 문서나 임의의 객체들에 대한 접근조종이다. 그 방법은 자료기지객체에 대한 접근조종과 류사하다. 의뢰기/봉사기프로그람들에서 XML은 SQL요구와 류사할수 있다. 즉 XML은 요구되는 자료를 지정하기 위하여 쓰인다. 자료기지봉사기가 보관된 자료와 봉사에 대한 접근을 제한하는것처럼 XML요구에 응하는 봉사기는 자기가 봉사하는 자료에 대한 접근을 조종할수 있다.

SQL에서 요구와 조종의 기본대상은 표(table)이다. 그러나 대부분의 자료기지봉사기들은 또한 더욱더 치밀한 조종을 제공하게 될것이다. 실례로 그런 봉사기들은 행, 렬 혹은 지어 세포에 대한 임의의 접근조종을 보장할수도 있다. 많은 봉사기들은 보기(view)라는 자료들의 임의의 결합에 대하여 조종을 실행할수 있다. 자료에 대한 임의의 접근조종이 언어나 스키마의 기능이라기보다 자료기지관리자의 기능이라는것을 알아 두라. 또한 자료가 자료기지관리자의 손에 있을 때에만 스키마에 결합된다는것을 명심하라. 자료기지관리자가 자료를 다 봉사할 때에는 자료의 무결성을 보존하기 위하여 믿음직한 경로들과 과정들이 요구될수 있다.

HTML에서와 같이 XML에서 접근조종의 기본대상은 문서이다. 이 목적으로부터 문서는 자료기지표와 류사하게 된다. 거의 모든 봉사기들이 일부 페지들에 대한 접근을 제한할수 있다. 이런 능력이 드물게 리용되지만 많은 봉사기들은 페지들에 대한 임의의 접근조종을 제공한다. 즉 이 봉사기들은 일부 사용자들에게 한페지에 대한 접근을 허용하면서도 다른 사람들에게는 허용하지 않는 능력을 가지게 된다. 실례로 Apache Web봉사기는

특정한 사용자들, 사용자그룹들, IP주소들 또는 주소/사용자쌍들의 이름 달린 문서들에 대한 접근을 경영인이 허락하거나 제한하도록 승인한다. 자료기지관리자가 같은 자료에 대한 여러가지 보기들을 지정함으로써 보다 치밀한 접근조종을 실행할수 있는것처럼 봉사기의 관리자도 역시 각이한 문서들을 만듦으로써 보다 치밀한 조종을 실행할수 있다.

그러나 태그들은 문서보다 더 세밀한 객체들을 상세히 서술하는데 쓰인다. 이것은 보다 치밀한 접근조종의 가능성을 제공한다. 자료기지관리자가 표보다 더 치밀한 접근조종을 보장하는것처럼 봉사기도 폐지보다 더 치밀한 접근조종을 보장할수 있다. 이것을 기어코 하려고 한다면 임의의 태그객체의 수준까지도 할수 있을것이다.

공정 대 공정인증

Web상에서 특히 전자상업거래응용프로그람들에서 의뢰기공정은 자기신원을 봉사기공정에 보여 주는것이 종종 필요하다. 믿을수 있는 제3자들이 이런 《성의》를 보여 주게 된다. 이러한 체계들에서는 인증서를 위조 또는 재현하지 못하도록 하는 방법으로 자료를 교환할수도 있다. 이러한 교환을 위하여 규약을 잘 작성한다. 이 규약들을 구조화된 자료에 서술한다. XML에서 이런 교환에는 두개의 스키마가 있다. 즉 하나는 인증서자체를 위한것이고 다른 하나는 인증서들을 요구하기 위한것이다.

XML의 한 변종인 authXML은 이런 프로그람을 위한것이다. 그것은 신원확인을 요구하기 위한 자료와 이 요구를 지원하는 증거를 위한 형식화들(format)을 정의한다.

공정 대 공정무결성

우의 경우와 마찬가지로 전자상업거래응용프로그람들에서는 거래를 수자식으로 서명하여 그 신원과 내용을 보여 줄수 있다. 이렇게 하자면 거래자체와 서명 및 인증서를 위한 태그들이 필요하다. 보안봉사표식달기언어(SML: Security Services Markup Language)는 기업 대 기업(B2B) 거래 및 기업 대 소비자(B2C)거래에 망라된 회사들사이에서 보안봉사를 공유하기 위한 공통언어를 제공한다.

권 고 사 항

1. **자료를 식별하고 태그로 표식하라.** 자료에 대한 태그들을 보존하라. 통신에 쓸모있고 또 리용되고 있는 한 메타자료는 무엇보다도 자료소유자가 리용하기 위한것이다.
2. **자료에 메타자료를 붙여 놓으라.** 자료기지관리자, 접근조종보관고, 암호기법, 신뢰응용프로그람과 체계들 및 신뢰경로들을 리용하라.
3. **의존하고 있는것을 확증하라.** 이것이 현대망세계에서 기본보안규칙이다. 객체서술에 의거하는 경우에 그 서술을 사용하고 있다는것을 확신하라. 숨겨 진 스크립트

가 없는 객체에 의존하는 경우 스크립트를 꼭 찾아 보라.

4. **믿음직한 원천에서만 태그들을 접수하라.** 한 원천의 태그와 자료들을 다 같이 중시해야 한다. 한 원천의 태그없는 자료를 접수하지 말며 태그없이 자료를 접수할수 없는 곳에서는 태그들이 있는 자료들을 접수하지 말라.
5. **예견되지 않은 태그들이 있는 자료들은 접수하지 말라.** 그 태그들을 넘기지 말라. 태그들을 벗기지도 말고 자료들을 넘기지도 말라.
6. **사용기록부와 실행기록부에 태그들을 포함시키라.** 이렇게 하면 사용기록부와 실행기록부의 무결성과 리용성을 높일뿐아니라 책임해명을 개선할수 있다.
7. **규정되여 있고 쓸모 있는 보안태그들을 사용하라.**
8. **응용프로그람개발자들과 적중한 표준, 절차 및 시행관리자들에게 이 권고사항들을 통보하라.** 이 대책들이 메타자료의 안전한 리용에 필수적이지만 그 리용과 조종은 흔히 다른 문제를 우선시하는 사람들의 손에 달려 있다.
9. **말단사용자들이 초래하는 결과에 집중하라.** 결국 응용프로그람의 보안은 말단사용자가 리해하고 수행하는것에 달려 있다.

결 론

HTML과 그와 류사한 메타자료언어들은 10년전에는 상상도 할수 없었던 각이한 수준의 운용호환성을 가져다 주었다. 인터네트에서 운용호환성이 있는 체계들의 수가 선형적으로 늘어 났다면 사용자들이 덕을 보는 그 가치는 기하급수적으로 늘어 났다. XML은 그 운용호환성을 보다 높은 단계로 끌어 올릴것을 기약한다. XML은 인터네트에서 의뢰기와 봉사기사이의 운용호환성을 창조하는데 도움을 줄뿐아니라 지적된 임의의 객체들과 공정들사이의 운용호환성도 개선하게 된다. XML은 자료의 의미와 목적을 그대로 전달함으로써 자료의 편의성과 가치를 높이게 된다. COBOL이 출현하기전까지는 그런 약속을 할 도구가 없었다. 이 약속은 충분히 실현될것 같고 또 큰 규모로 실현될수도 있을것이다.

그러나 임의의 도구와 마찬가지로 XML의 가치는 대체로 그것을 리용하는 사람의 기술기능수준에 달려 있다. 임의의 착상과 마찬가지로 XML의 가치는 그에 대한 리해에 달려 있다. 임의의 새 기술과 마찬가지로 XML의 가치는 공포와 무식으로 인하여 충분히 발현되지 못할수도 있다.

임의의 새로운 도구를 쓸 때와 마찬가지로 XML의 능력과 제한성에 대하여 리해해야 한다. 정보기술에서는 제한성에 대한 충분한 고려가 없이 도구들을 사용하는것과 같은 많은 문제들을 야기시키는 현상은 거의 없었다.

XML의 리용은 종종 정보보안전문가들의 시야밖에 있었지만 누구도 XML의 제한성, 오용 및 람용에 대하여 우려하지 않을것이다. XML의 제한성, 오용 및 람용으로 인하여 기업이 손실을 당하는 경우에는 그에 대하여 우리가 책임을 지게 될수도 있을것이다. 이런 제한성, 오용, 람용으로 인하여 이 중요한 견해가 은을 내지 못하게 되면 우리모두는 그로 인하여 더욱 난처하게 될수도 있을것이다.

제３０장. XML과 정보보안

사무엘 씨 엠씨클린토크

정보기술은 나날이 변해 가며 세계는 거의 매해 정보시대의 새로운 《성배》를 받아안게 된다. 바로 그것이 확장표식언어(XML: eXensible Markup Language)이다. XML의 심장부는 복합자료구조들을 서술할수 있는 본문에 기초한 간단한 언어이다. 그 간단성으로 하여 거의 모든 콤퓨터들이 XML을 리용할수 있으며 모든 형태의 망들이 그것을 전송할수 있다. XML은 거의 모든 판매업체들로부터 매우 광범한 지원을 받아 거의 모든 콤퓨터체계들이 현존하부구조를 크게 수정하지 않고도 XML을 조작할수 있게 하였다. 그렇다면 무엇이 문제인가.

기본문제들은 변하지 않았다. 인터네트는 이전처럼 불안전한데 기술은 무서운 속도로 발전한다. 일부 사람들은 오유를 범하고 다른 사람들은 정보를 훔치거나 파괴한다. 지금까지 구축된 모든 콤퓨터체계들에 GIGO(garbage–in garbage–out 즉 불완전한 자료를 입력시키면 결과도 불완전하다는 말)가 아직도 그대로 적용된다. XML은 이 모든것을 조금도 변화시키지 못하였으며 오히려 또 하나의 람용의 길을 열어 놓는다. XML은 전진하는 보안사업에 망라될 또 하나의 대상으로서 몇가지 보안약점도 보충하고 있다.

XML의 많은 정보보안문제들이 현존하는 문제들과 공통적이라는 사실은 XML을 현행보안실천에 쉽게 적응시킬수 있게 한다. 또한 XML은 바로 그 본성으로 하여 언어의 《확장》들을 만들어 암호기법과 같은 각이한 XML보안해결책들을 명확하게 제시할수 있게 한다. 주요판매업체들은 이미 XML환경보안을 설계하였으며 XML에서의 암호화기법과 수자식서명의 새로운 표준들을 제기하였다. 그러나 최근의 해결책들은 결코 완성된것들이 아니다. 프로그람작성자들, 자료기지관리자들 및 경영자들은 XML이 자료를 보다 쉽게 읽고 조직하고 보급할수 있게 하며 임의의 기존자료들을 효과적으로 바꾸지 않으면서 알맞는 보안을 계획한다는 사실에 주의를 돌려야 한다.

XML은 우리의 모든 정보기술을 리용하면서 계속 빠른 속도로 발전할것이다. 래일의 정보보안전문가들은 XML이 리용하는 자원을 보존해야 할것이다. 이 전문가들은 또한 그들이 사용하는 많은 보안도구들에 XML이 통합되는것을 보게 될것이다. 그러므로 정보보안전문가들은 XML과 XML응용프로그람보안문제들을 리해할 필요가 있다.

XML기초

XML과 XML보안문제들을 리해하자면 그 배경을 좀 알아 두는것이 필요하다. 정보보안전문가들에게는 이것이 자기들의 적을 알게 되는것으로 보일수 있는가 하면 기술적으로 초래된 정신분렬증에로 또 한걸음 들어 가는것으로도 보일수 있다.

왜 HTML이 아닌가

HTML(Hyper Text Markup Language)는 World Wide Web의 기초의 하나이다. HTML은 특히 단순하고 리용하기 쉬우며 세계에서 가장 성과적인 출판언어의 하나로 되였다. 지어 프로그람작성자가 아닌 사람도 HTML의 기초원리들과 문서를 정의하는 코드나 《태그》들을 배울수 있으며 Web싸이트들을 만들수 있다. 그러나 HTML은 자기 성과의 희생물로 되였으며 HTML리용의 편의성은 Web의 성장과 그에 대한 기대로부터 나온 제한성들에 직면하게 되였다. 즉 그에 대한 기대로부터:

- HTML은 확장될수 없으므로 특정한 요구들을 위한 태그들을 정의할수 없다. 만일 그렇지 않다면 각이한 열람기판매업자들은 열람기들의 새로운 기능확장들을 고안하여 개발자들에게 무서운 두통거리를 제기할것이다.
- HTML은 문서의 내용이 아니라 형식만을 서술함으로써 Web상에서 특정한 내용을 발견하는데 더 큰 난관을 조성한다.
- HTML은 개별적요소들을 의미적으로 표식할수 없으므로 매 요소가 무엇을 의미하는지(즉 집주소와 전자우편주소사이의 차이) 지적할수 없게 한다.

Web에 기초한 정보의 확산은 그 모든 정보를 식별할 능력이 우리에게 없는것으로 하여 실효성이 없는것으로 되고 있기때문에 HTML의 이 제한성들은 사실상 Web의 속도를 늦추고 있다. WWW으로 알려 진 이른바 《빛속도》망의 속도는 기여 가는 속도로 떨어 지고 있다. 특정한 싸이트뿐아니라 제품의 가격 또는 빛갈과 같은 그 싸이트안의 특정한 정보도 있을수 있는 선택의 경우가 지나치게 많은 사정으로 탐색하는데 시간이 더 많이 걸린다.

SGML: 그 모든것의 시원

HTML이 일으키는 문제들을 리해하기는 어렵지 않았다. 1996년 W3C(the World Wide Web Consortium)는 해결책을 찾기 위하여 어머니언어 즉 SGML(the Standard Generalized Markup Language)에로 소급하여 보았다. 대부분의 사람들은 HTML이 SGML의 아주 단순한 응용이라는것을 모르고 있다. SGML은 수많은 쏘프트웨어판매업체들이 지원하는 보편적인 표준인바 이 표준은 자료를 표현하는 방법이 아니라 자료자체를 서술한다. SGML은 더 구조화된 환경을 제공한다. 임의의 SGML문서는 임의로 겹쳐 쓰이여 다른 문서를 포함함으로써 보다 단순한 문건들로 복합문서들을 만들수 있게 한다.

SGML에서 유일하게 문제로 되는것은 SGML이 500페지가 넘는 설명서(표준 및 요구조항들)로서 너무도 일반적이고 너무도 복잡하여 대부분의 Web열람기들이 처리할수 없다는것이다. 그에 대한 방도는 제한과 부단한 적용이 필요한 HTML을 확장하지 않는것이였다. 그리하여 사용자들이 자기의 표식달기언어를 만들수 있게 하는 흐름식메타언어인 SGML의 부분모임을 창조하는 과정에 새로운 언어인 XML이 파생되였다. XML의 설명서는 SGML의 본래의 500페지보다 훨씬 더 다루기 쉬운 50페지로 제한되였다. 그러나

XML은 누구든지 령으로부터 표식달기언어를 창조할수 있는 규칙들로 구성되여 있다. XML은 또한 HTML이 새로운 메타언어에 조화될수 있게 구성된다(그림 30－1을 볼것).

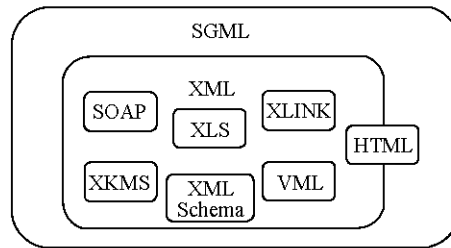



그림 30－1. SGML과 XML의 구조

XML의 장점들

많은 회사들이 기대를 걸고 XML에 편승하고 있다. XML은 많은 장점들을 제공하고 있지만 이것들가운데서 많은것들이 HTML에는 없었다. 이런 장점들은 다음과 같은것들이다 :

- **단순성** XML은 흔히 사람과 콤퓨터들이 쉽게 읽고 리해할수 있으며 콤퓨터로 쉽게 처리할수 있다. XML은 또한 복합자료구조들을 표현할수 있다. XML은 분산쏘프트웨어기술(CORBA와 DCOM과 같은)보다 배우기 쉬우며 개발시간이 적게 든다.
- **열린표준** XML은 W3C의 열린표준이며 세계의 거의 모든 중요한 쏘프트웨어개발자들이 XML을 인정한다. Microsoft, Oracle 및 IBM은 《아침해가 어디서 떠오르는가에 대해서는 견해일치를 보지 못할》수 있으나 자기들의 쏘프트웨어제품에서 XML열린표준만은 일치하게 지원한다.
- **자료서술** XML은 메타자료 또는 정보에 관한 서술자료를 쉽게 제공할수 있게 한다. 이것은 자료채취 또는 보다 능률적인 탐색엔진들의 실천가능성을 열어 주어 소비자가 정보나 정보산생자를 찾을수 있게 도와 준다.
- **출판편리성** XML의 가장 큰 장점들중의 하나는 설계로부터 내용을 분리할뿐아니라 그 반대과정도 수행하는 능력이다. 내용관리는 타자기시대로부터 힘을 넣은 문제로 되여 왔으며 문서들이 수자식하부구조와 뒤섞이게 되면서 더욱 중요하게 되였다. XML은 내용을 다치지 않으면서 문서의 형식을 바꿀수 있게 하며 또 설계를 다치지 않으면서 내용을 바꿀수 있게 하는 중요한 해결책을 제공한다.

XML나트와 볼트

XML은 누구든지 령으로부터 표식달기언어를 창조할수 있게 하는 규칙과 규약들로 이루어 진다. 결과 XML문서를 만들 때 문서작성자는 자기의 요소들을 만들고 그것들에

자기가 좋아 하는 이름들을 붙여 준다. 이런 식으로 XML은 승용차부속품명세나 면담자명단과 같은 거의 모든 문서형태들을 서술하는데 쓰일수 있다.

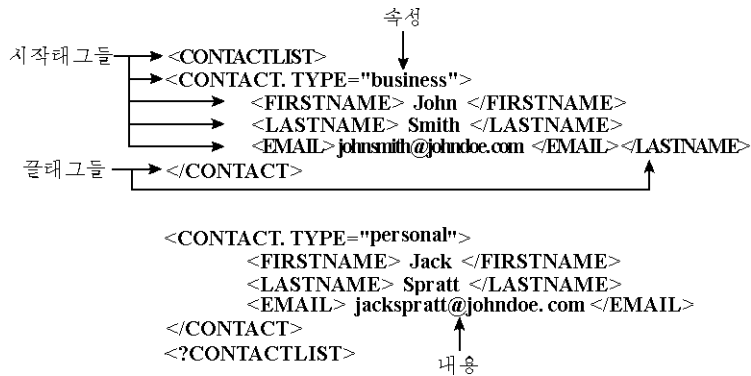



그림 30－2. XML의 기초문장론

그림 30－2에서 보는바와 같이 XML의 문장론은 아주 쉬우므로 지어 프로그람전문가 아닌 사람들도 몇시간안으로 태그들을 개발할수 있다. 이 실례는 또한 형식이 잘된 문서작성에 필요한 기본규칙들을 보여 준다. 형식이 잘된 문서는 그 문서가 처리되도록 하는 규칙들의 최소모임에 준한것이다. 그림 30－2의 실례는 XML에 대한 다음과 같은 규칙들에 준하고 있다. 즉 :

- **문서요소** 매 문서는 오직 하나의 최상위준위요소를 가져야 한다. 실례의 문서요소 또는 뿌리요소는 《CONTACTLIST》(면담자명단)이다.
- **요소겹쳐쓰기** 한 요소가 다른 요소안에서 시작되면 역시 그 요소안에서 끝을 맺아야 한다. 이 실례에서 한 행이

  <EMAIL> johnsmith @ johndoe.com</CONTACT></EMAIL>

  과 같이 씌여 졌으면 :</EMAIL>끝태그가 </CONTACT>끝태그앞으로 나와야 하기때문에 그것은 유효하다고 볼수 없을것이다.
- **시작태그와 끝태그** 매개 요소는 시작태그와 끝태그를 다 가져야 하며 요소의 이름은 해당한 끝태그의 이름과 정확히 일치해야 한다. 요소이름들에서는 대소문자가 정확히 구별되여야 한다.

이 실례는 XML이 아주 단순하지만 여러 면에서 엄밀하다는것을 말해 준다. 그러나 이것은 하나의 문제거리로 되는것이 아니라 XML의 실제적인 통합능력의 하나를 의미하는것이다. 다시 말하여 그 통합능력의 하나가 그대로 다 작용하도록 하기 위하여 누구나 다 해당한 규칙들을 준수하여야 한다.

문서형식정의

리해할수 있는 태그들조차 그것들을 요구하는 사람들에게 알려 지는 경우에야 비로소 실용적인것으로 된다. 공통적인 문서형식을 가지고저 하는 사용자그룹들은 XML에서 또 하나의 가치 있는 도구 즉 문서형식정의(DTD)를 리용한다. XML의 이 측면은 정보교환을 위한 업계의 표준을 쉽게 정의할수 있게 한다. 그러므로 우의 실례는 그림 30－3에서 보는바와 같이 DTD다음에 올수 있다.

```
헤더          → <?xml version ="1.0"?>

문서형태      → <!DOCTYPE CONTACTLIST
 선 언             [
                   <!ELEMENT CONTACTLIST (CONTACT)*>
                   <!ELEMENT CONTACT (FIRSTNAME, LASTNAME, EMAIL)>
요소형태를         <!ATTLIST CONTACT type (business|personal) #REQUIRED>
정의하는    ——→    <!ELMENT FIRSTNAME (#PCDANA)>
Markup선언         <!ELMENT LASTNME (#PCDANA)>
                   <!ELMENT EMAIL (#PCDANA)>
                   ]
               >
```

그림 30－3. XML header가 있는 DTD

또한 DTD들을 리용하여 아주 위력한 확인을 진행할수 있는것이다. 그림 30－3의 DTD에서는 요소 CONTACT를 이루는 요소들사이에 있는 반점들을 리용하여 그다음(자식)요소들의 《순서》형식을 지적하게 된다. 그러므로

```
<!–Invalid element–>
<CONTACT>
     <LASTNAME> Doe </LASTNAME>
<FIRSTNAME> Jane </FIRSTNAME>
     <EMAIL> janedoe @ johndoe.com </EMAIL>
</CONTACT>
```

와 같은 요소를 첨부하려고 하는 경우에 새끼요소들의 순서가 DTD에 표시되여 있지 않으므로 그 요소는 무효한것으로 간주될것이다. 새끼요소를 생략하거나 혹은 같은 새끼요소형식을 한번이상 포함하는것도 또한 무효한것으로 간주될것이다.

XML이 단순하며 문서형식들을 정의할수 있기때문에 XML은 대화형영업프로그람을 작성하는데 필요한 중요한 프로그람작성문제들을 해결할 잠재력을 가진다. XML요소들과 문서구조의 다목적모임은 XML응용프로그람 혹은 XML어휘로 알려 져 있다. 재정, 보건, 화학 및 신문업과 같은 기업들은 그 기업성원들을 위한 자기들의 기업용XML응용프로그람들을 작성하는 사업에 이미 큰 규모로 착수하였다. 실례로 CML(Chemistry Markup Language)와 OFX(Open Financial Exchange)를 들수 있다.

기타 XML도구

특정한 산업그룹 혹은 문서류를 위한 XML응용프로그람들을 작성하는것외에 임의의 XML문서형식안에서 쓰일수 있는 XML응용프로그람 또는 표준들은 끊임없이 개발되고 있다. 이 응용프로그람들은 XML문서들을 보다 쉽게 만들며 형식화하고 보안할수 있게 한다. 다음과 같은 몇가지 실례들이 있다.

- **XLink.** 새로운 《XML련결언어》는 다중련결목표들을 허용하므로 HTML련결기구보다 휠씬 더 위력한것이다.
- **XSL.** 《확장스타일쉬트언어》(eXtensible Stylesheet Language)는 XML문장론을 리용하여 강력한 문서스타일쉬트를 만들수 있게 한다.
- **XML스키마.** XML스키마에 대한 공식적인 개념은 2001년 3월에 W3C에 의하여 발표되였다. XML스키마는 DTD들을 기록하는데서 보다 강력한 대안으로 된다.

XML의 보안문제

인터네트에서와 마찬가지로 XML이 설계될 때도 정보보안은 일차적인 관심사로는 물론 지어 이차적인 관심사로도 될수 없었다. 《보안》이라는 말은 XML에 대하여 그것이 권고되던 초기에 프로그람작성실례로 겨우 명목상으로 출현하였다. 그러나 XML은 자료를 보다 쉽게 읽고 조직하고 보급할 전망을 안겨 준다.

XML은 파국적인 기술인가

임의의 새 기술에서 중요한 문제거리의 하나는 그 파국적인 작용의 잠재력이다. 정보보안전문가들은 완성된 제품들을 좋아 하는 경향이 있으며 안전하고 불변적인 환경속에 있을 때 제일 위안을 느낀다. XML은 결코 완성된것이 아니며 거의 매달 새로운 표준을 도입하게 된다. XML은 또한 인터네트의 전반적모습뿐아니라 다른 많은 기업 및 자료기지응용프로그람에도 변화를 가져 온다.

대체로 가장 큰 변화는 HTML에 기초한 기술과 규약에서 생긴다. 이 기술과 그것과 련관된 기반에는 결함들이 있다. 그러나 이 결함들은 체계관리자나 또는 정보보안전문가가 리해할수 있는것들이였다. 이 기반들에 대한 현존규약들은 일정한 한계까지는 아주 훌륭하게 작용한다.

XML이 주는 영향의 가장 큰 실례는 HTML이 자기자체만으로는 앞으로 더는 중시되지 않으며 XML안에서 재형식화되는것이 주목할만하다는것이다. 본질상 XML은 HTML의 개발을 그자체의 령역까지로 종식하였으며 HTML이 중요함에도 불구하고 그것을 어휘상태로 제한한다.

장황성과 파일크기

XML표식붙이기는 장황해 질수 있다. XML은 본문형식이며 태그들을 리용하여 자료의 한계를 정한다. 이것으로 하여 XML파일들은 대부분 2진형식보다 언제나 더 큰것이다. 앞의 실례들에서 XML태그들은 파일의 크기를 쉽게 3배로 늘일수 있다. XML제안자들은 디스크공간이 이전만큼은 비싸지 않으며 자료를 정확하고 신속하게 압축하여 송신하는 많은 방법이 있다는것을 강조하고 있다.

파일크기확장의 이 새 측면은 보상될수 있지만 그것을 잘 계획해야 하며 어떤 부차적인 실행요인으로 대하지 말아야 한다. 어떤 회사들은 XML로 구축된 테라바이트이상의 큰 자료를 전송하고 있다. 파일크기가 최소한 40~50%만 확장되여도 이런 큰 자료기지들에 어느정도 값 비싼 큰 영향을 줄수 있다. XML에로의 이행이 계속되고 있으므로 각급 정보기술실무자들과 경영자들은 이런 보다 큰 체계를 위한 기억공간 및 대역너비문제들을 중시해야 한다.

다시 인터네트에 대하여

XML은 인터네트를 리용하는 기업응용프로그람들가운데서 급속히 공통언어로 되여 가고 있다. XML은 준비되는 차제로 쉬운 구매, 은행업 및 기타 기능들을 감당해야 한다. 그러나 인터네트는 여전히 불안전하며 XML은 그것을 개선하지 못할것이다. 사실 사람들은 인터네트로 전달되는 모든 자료를 읽고 리해하기 쉽게 하는 방향에서 XML을 의도적으로 리용하고 있다.

W3C와 함께 거의 모든 주요판매업자들은 이 문제로 하여 XML을 받아 들이려는 자기들의 노력이 수포로 돌아 갈수 있다는것을 알았다. 이 문제는 본질상 잘 알려 진 두 보안문제 즉 비밀성과 인증에 귀착된다. 암호화는 보다 신중하고 사적인 자료의 비밀을 보장하기 위하여 필요한것이다. 다시 말하여 이 문제는 바로 세부준위에서 일어 날수 있는 문제로 된다. 실례로 문서에서 정보를 끌어 내는 사용자는 볼 필요도 없는 정보를 호출할수도 있다. 수자식서명들은 확실성, 무결성 및 부인방지를 보장하기 위하여 필요하다.

우선 주요판매업체들은 보안해결책들을 세워 XML응용프로그람들에 대한 암호화 및 수자식서명을 보장하였다. 그때로부터 주요판매업체들과 각이한 실무그룹들은 XML에서의 새 암호화와 수자식서명요구들에 대한 제안들을 신속히 추적하고 있다. 즉 :

- **암호화** 2001년 3월에 W3C는 XML암호화에 필요한 기술설명서를 발표하였다. 설명서에 의하면 W3C실무그룹의 임무는 《암호화/복호화내용(XML문서와 그 부분을 포함하는) 그리고 (1) 암호화된 내용, (2) 해당한 수신자가 그것을 복호화할 수 있게 하는 정보를 나타내는데 쓰이는 XML문장론을 위한 공정을 개발하는 것》이였다.
- **수자식서명들** XML서명요구사항(지금은 W3C의 두번째 건으로 간주되는)은 XML열쇠관리기술설명서(XKMS)와 함께 처리되고 있다. VeriSign, Microsoft, Baltimore Technologies, Citigroup, IBM, IONA Technologies, PureEdge, Reuters를

비롯하여 몇개의 주요 쏘프트웨어판매업체들이 2001년 3월에 XKMS요구사항들을 제출하였다.

DTD와 새로운 보안문제

임의의 새로운 기술도입에서와 마찬가지로 XML의 통합은 공격, 파괴 및 람용당하게 될 보안허점들을 뚫어 놓게 될것이다. 아마도 가장 큰 보안위협은 XML스키마, DTD들 그리고 지어는 XSL스타일쉬트(stylesheets)들의 계획적인 및 자연발생적인 교체에서 오게 될것이다. 산업그룹속에서 응용프로그람 또는 어휘의 창조는 모든 응용프로그람의 기초로 될 하나의 XML응용프로그람이 있게 될것이라고 가정할수 있게 한다. 내부와 외부에서 사용하기 위하여 《표본》 DTD들 또는 스타일쉬트들을 회사들이 사용할것이며 많은 경우에 요구하게 될것이라고 가정하는것 역시 론리적인것이다. 사소한 변화도 DTD에서 치명적인 오유를 산생할수 있으며 XML처리과정을 큰 규모로 멈춰 세울수 있다. 이런 공격은 정교로울 필요가 없다. 크래커(cracker)는 선택속성을 필요한 속성으로 변화시킬수 있으며 한 회사가 이런 작은 《무해한》 오유를 찾느라고 여러 시간을 허비하는것을 보면서 깨고소하게 웃을수도 있다.

한다하는 보안전문가가 자료의 보안을 위하여 기정속성이나 DTD에 의거하는 경우에는 어떻게 되겠는가. 자그마한 변화라도 특권자료의 엄청난 분량을 로출시킬수도 있다. 접근조종을 위하여 각이한 보안제품들이 XML에 의거한다면 어떻게 되겠는가. 자그마한 오유가 망으로부터 회사전체를 격리시킬수 있으며 또는 망봉사로부터 제외시키려고 하는 바로 그런 사람들에게 접근할수 있는 조건을 제공할수도 있다.

DTD들은 또한 다른 방법으로 리용될수도 있다. XML문서의 머리부(header)가 하나의 URL을 보유하여 망상에서 그밖의 DTD에로 경로를 설정하는 경우에 의뢰기는 DTD에 접근하여 XML객체를 평가해야 한다. DTD호스트봉사기가 방화벽뒤에 있을 경우에 의뢰기와 봉사기사이에 통신이 일단 이루어 지면 방화벽은 격파될수 있다.

이 모든 공격들 즉 문제거리들은 콤퓨터체계들이 파괴되는 다른 방법들과 관계되는 아주 단순한것들이다. 차후의 해결책들이 의심할바 없이 발표되여 새로운 보안이 각이한 XML도구모임들에 도입되지만 XML의 열린특성은 이 덜 정교한 공격들이 계속 문제거리로 되게 할것이다. 특히 알맞는 대책을 세우지 못하여 자기 자료들을 보존하지 못하는 보다 풋내기회사들의 경우에는 더욱 그렇게 된다.

XML계렬, 이붓자식 및 사생아

XML은 틀림없이 기술의 계렬(family)이지만 특정한 과업을 위한 모듈과 응용프로그람의 끊임없는 개발은 수많은 의혹을 자아내고 있다. XML암호화 즉 XSL 또는 Xlink에 대한 일부 새로운 기술설명서들이 지금 잘 작성되여 있다. 그러나 주요 쏘프트웨어판매업체들로부터 금융기관에 이르기까지의 주요 련관기관들은 아직도 토론해야 할 많은 문제를 안고 있다. 다른 기술설명서들과 권고안들이 바로 지금 공개되고 있으며 더 많은것들이 가까운 몇해안에 개발될것이다. 물론 이미 XML을 지원하는 쏘프트웨어판매업자들

도 아주 많은것이다. 틀림없이 매개 새로운 모듈 또는 응용프로그람이 《공식적》이기때문에 의심할바 없이 XML에 새로 보충된것들을 지원할 갱신된 쏘프트웨어들은 아주 많은것이다.

XML을 위한 새로운 쏘프트웨어가 개발되여 XML이 현존 제품들에 보충됨에 따라 《강화된》응용프로그람을 될수록 빨리 시장에 내놓으려는 움직임으로 하여 보안허점들은 커질것이다. 실례로 XML의 통합이후에 열람기응용프로그람 및 자료기지응용프로그람과 함께 발전한 보안문제들을 생각해 보라. 이런 경향은 가까운 앞날에도 계속될것 같다.

모든 요구, 모듈 및 응용프로그람들이 XML에 적용되면서 그 분야가 모두 혼란되여 그 시도전반에 약간의 위험을 또 주게 될것이다. 또한 이것은 W3C 또는 각이한 산업그룹들이 모르게 진행될수는 없었다. 400개이상의 성원기관들로 구성된 업계제휴단체인 RosettaNet는 각이한 XML응용프로그람들의 수렴과정에 대한 청원을 최근에 제기하였다. 그러나 400성원기관이 XML계를 대표할수는 없고 모든 관계단체들이 간섭하므로 세계는 좀 어려운 과정을 거쳐 이 수렴을 실현하지 않으면 안되는것이다.

결　론

XML을 위한 각이한 표준, 요구 및 묘듈에 기초하여 지금 많은 작업이 진행되고 있으며 이 사업은 높은 속도로 성숙되여 가고 있다. 계속 전진하고 있는데 오유는 범하지 말라. XML은 이미 존재하고 있다. XML은 정보기술을 통하여 회사, 산업별 및 세계적규모로 퍼져 나가고 있다. 그리고 XML은 전자출판, 자료기지보관, 전자문서의 교환 및 응용프로그람통합에 큰 영향을 주고 있다. 그러므로 정보보안에 망라된 경영자들을 비롯한 각급 경영자들은 《성배》로 알려 진 XML의 특성을 파악하는것이 중요하다. XML확산의 이상한 측면의 하나는 이 《성배》를 드는 특전을 누리는 경우에는 한사람이 아니라 모든 사람들이 《성배》를 들어야 한다는것이다. 성공하기 위하여 그리고 WWW상에서와 전자상업거래에서 XML의 전망을 모든 사람들이 알도록 하기 위하여 사용자가 XML에 기초하여 입력할것을 XML은 흔히 요구하는것이다. XML이 널리 리용되면서 정보의 보다 빠른 공개, 주문의 보다 빠른 처리 그리고 문건의 보다 빠른 탐색에서 사람들은 혜택을 입게 된다. 물론 이 성공의 큰 요인은 XML통합 및 사용이 안전하게 진행될수 있겠는가에 따라 좌우될것이다.

보안해결책으로서의 XML

XML을 위하여 처리되여야 할 모든 보안문제들외에 앞에서 고찰하지 않은 경향 즉 XML이 보안해결책의 하나로 리용되고 있다는것을 민감한 보안전문가, 프로그람작성자 또는 경영자는 실감하기 시작할수도 있다. 보안은 보건사업이나 자동차관리와 다를것이 없다. 다시 말하여 보안은 자체의 독특한 어휘와 자료조직방법을 가지고 있다. XML은 정보보안을 위한 일반문서의 기틀을 보장하는데 쓰이게 될뿐아니라 응용프로그람들과 콤

퓨터체계들사이에서 각이한 보안과업들을 통합하는데도 쓰이게 된다.

사람들은 Microsoft Exchange와 같은 보안련관프로그람들의 각이한 측면에서 이 경향을 이미 파악하기 시작하였다. 이 경향이 지속되면서 보안전문가들이 XML의 기초원리들을 각이한 보안해결책들에 리용하는 방법을 리해하는것은 더욱 중요하게 될것이다. 왜냐하면 XML이 각이한 보안구성요소들속에서 결합력 있는 구성요소로 될수도 있는 가능성이 충분하기때문이다.

이제부터는 어디로 가야 하는가

XML세계는 요구성이 높은 세계이다. 그러므로 이 장에서는 XML과 XML보안문제를 폭 넓게 취급하였다. XML을 적용하여 가장 충분하고 안전한 응용프로그람을 작성하며 XML에 의존되는 자료를 구축하려면 프로그람작성자들, 경영자들 및 보안전문가들이 광범위한 문제들에 정통하여야 한다. 스타일쉬트, DTD, 자료나무 및 초련결구조들은 수자식세계의 보다 견고하고 보다 리용가치 있는 하부구조에서 모두 보편화되게 될것이다. 방어는 훌륭한 보안방책들을 유지하기 위해서뿐아니라 기술을 부단히 갱신하기 위해서도 필요하게 된다.

보다 많은 정보를 위하여 XML에 대한 최신정보와 소식을 제공하는 Web싸이트변종들이 있다. 고찰하기 좋은 곳은 W3C(월드 와이드 Web협회)Web싸이트 즉 WWW.W3.org이다. 또한 임의의 검색엔진에서 《XML》을 찾게 되면 곧 그에 대한 많은 정보를 볼수 있다. 사람들은 그 XML이 시간이 감에 따라 보다 많은 정보를 더 빨리 보다 더 정확하게 검색하는 그 공정을 발전시켜 나가기를 바랄뿐이다.

제３１장. 관계형자료기지응용에서의 수자식서명

마이크 아 프레보스트

공개열쇠암호화와 공개열쇠기반(PKI)이 인터네트의 보안기초로 인정되면서부터 새로운 보안제품들이 등장하고 있다. 그러나 이러한 제품들의 대부분은 응용자체보다도 상업적인 응용을 위한 기반과 관련한 문제들을 해결하는데 기본을 두고 있다. 실례로 가상개별망(VPN)제품들은 인증서에 기초한 인증과 공개열쇠에 기초한 열쇠교환을 지원하기 시작하였다. SSL은 Web에서 사적비밀과 인증을 위한 표준이다. 이러한 류형의 기술들이 절실히 필요한데 그것들은 모두 고도로 전용화되여 있으며 응용에서는 그러한 기술들이 눈에 보이지 않게 되여 있다.

수자식서명기술의 성격과 자료기지구동형응용에서의 그 리용은 일정한 정도의 응용통합을 요구한다. 수자식서명의 광범한 리용에서 일차적인 기술적난점이 바로 통합단계이다. PKI프로그람작성은 그 복잡성으로 하여 그것을 개발해 나가는 몇사람만이 알고 있는 《미지의 기술》(black art)로 남아 있다. PKI통합개발과제는 많은 응용프로그람소유자들에게 너무나 비싸고 위험한것으로 인정되여 있다. 그리하여 기관들은 복잡한 통합을 실행하지 않고 응용에 보안기능을 추가하는 방향으로 초점을 돌리는것 같다. 그러나 기반보안으로부터 응용보안에로의 이행에서는 수자식서명과 같이 보안기능을 응용 그자체에 더 쉽게 통합할수 있는 자료보안제품의 류형이 늘어 나고 있다.

이 장에서는 수자식서명기능을 관계형자료기지에 통합시키는데 필요한 내용들을 설명한다. 먼저 수자식서명의 개념을 설명하고 수자식서명이 응용보안방책에서 노는 역할, 관계형자료기지응용이 다른 환경들과 차이나는 리유, 여러가지 통합방법들의 일부 난점들에 대하여 설명한다. 끝으로 관계형자료기지에 보관된 자료를 수자적으로 서명하는 응용일반해결방법을 고찰한다. 여기에서는 수자식서명을 응용에 통합할수 있는 아주 쉬운 방법을 제공한다.

수자식서명의 개념

관계형자료기지에서 수자식서명은 자료무결성 또는 부인방지(례로서 원본의 증명)를 보증하는데 널리 리용된다. 수자식서명은 의미적으로는 문서서명과 류사하다. 그러므로 수자식서명은 문서의 인쇄, 서명, 전달, 보관의 필요성을 완전히 제거하거나 감소시켜 업무공정을 합리화하는데 리용된다. 수자적으로 서명한 문서의 서명자를 유지하는 합법적인 체계에서는 모든 문제들이 구체화되여 가고 있다.

수자식서명이 응용준위의 보안을 실현하는데서 필수적인 하나의 항목이라는것을 강조한다. 체계보안을 실현하는데서는 수자식서명과 함께 암호화, 인증, 권한부여, 접근조종, 방화벽, 침입탐지와 같은 다른 기술들도 중요하게 리용된다. 그러나 수자식서명은 다른 보안기술들로는 해결할수 없는 중요한 보안봉사를 제공한다.

트랜잭션의 분석

응용보안을 론할 때에는 《트랜잭션》(transaction: 1.외부거래기록을 위하여 말단 등에서 생성하여 콤퓨터체계로 전송되는 자료, 2.자료기지에 대한 조회나 갱신조작의 렬로 구성되는 처리의 기본단위–역주)이라는 용어가 자주 리용된다. 이 용어는 재정거래나 기업거래를 련상시키는 매우 애매한 용어이다. 때때로 《문서》(document)라는 용어도 리용된다. 당면한 목적에서 트랜잭션(또는 문서)은 응용에 의하여 보관되는 자료에 대한 변경으로 귀착되는 응용프로그람과 사용자사이의 어떠한 교환을 의미한다. 자료기지응용에서 트랜잭션자료는 관계형자료기지에 보관된다.

그림 31－1에서와 같이 트랜잭션은 4단계로 나누어 진다. 매개 단계에는 고유한 보안요구가 있다. 그림에서는 응용준위의 보안을 실현하기 위하여 수자식서명이 어떻게 리용되는가를 보여 준다. 이 단계들의 순서는 응용프로그람구성방식에 따라 차이날수 있다.

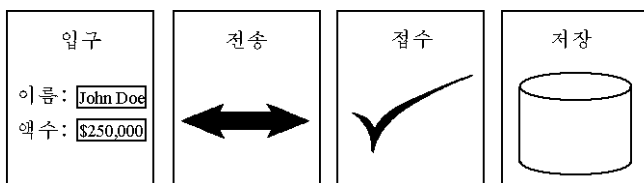



그림 31－1. 트랜잭션의 4단계

1단계: 자료입력 트랜잭션은 자료를 동반하므로 자료가 어디서든 시작되여야 한다. 이것은 사용자가 자료를 입력화면에서 건반으로 입력한다는것을 의미한다. 이 단계에서 응용프로그람은 보통 자료확인 즉 요구되는 모든 자료마당이 응용프로그람에 리해될수 있는 형식으로 되여 있는가 하는것만을 고려한다. 응용프로그람은 또한 어떤 사용자가 자료입력화면에 접근하는것을 막을수 있어야 한다.

2단계: 자료전송 많은 응용프로그람에서 트랜잭션자료는 망을 통하여 중심응용프로그람봉사기 또는 자료기지봉사기에 전송된다. 응용프로그람은 전송도중에 트랜잭션자료가 변경되지 않는다는것을 담보해야 한다. 그리고 트랜잭션자료에는 신용카드번호 또는 다른 사적비밀정보와 같은 중요한 정보도 포함될수 있다. 또한 응용프로그람은 트랜잭션자료가 의도한 목적지에 전달되고 있다는것을 보증하여야 한다. SSL구약의 Web기반응용에 광범히 리용되자면 이러한 요구들을 만족시켜야 한다. VPN기술도 역시 이러한 봉사들을 제공할수 있다.

3단계: 접수 처리과정의 어떤 시점에서 응용 또는 응용프로그람봉사기는 트랜잭션을 《접수》한다. 즉 트랜잭션은 필요한 모든 요구에 맞게 처리된다. 트랜잭션접수과정은 몇개의 요소들을 동반한다.

- **자료확인** 요구되는 모든 마당들이 응용프로그람에 리해될수 있는 형식으로 입력된다.
- **무결성** 자료는 응용프로그람 또는 자료기지봉사기로 전송되는 도중에 변경되지

않는다.

- **인증** 사용자의 신원은 정확히 설정되여 있다.
- **권한부여** 인증된 사용자는 이 트랜잭션을 진행할수 있는 권한을 가진다.

4단계: 보관 트랜잭션은 자료기지에 보관된 자료에 대한 변경으로 귀착되는 사용자와 응용프로그람사이의 호상작용으로 정의되기때문에 자료는 반드시 보관되여야 한다. 많은 경우에 어떤 트랜잭션은 새로운 자료가 자료기지에 씌여 질것을 요구한다. 또한 어떤 트랜잭션들은 이미 있는 자료를 변경시키기만 한다. 어느 경우에나 응용프로그람은 기억된 자료가 변경되거나 파괴 또는 부당한 사용자가 변경하거나 파괴하거나 볼수 없게 보관될 필요가 있다. 이러한 공격들은 흔히 강한 접근조종절차와 좋은 여벌복사계획에 의하여 방지될수 있다.

증명 대 방지

앞의 설명에서 생략된것은 트랜잭션보안요소이다. 접수단계(3단계)에서 다음의것을 알수 있다.

- 요구되는 모든 자료들은 접수할수 있는 형식으로 입력되여야 한다(확인).
- 자료는 전송도중에 변경되지 말아야 한다(무결성).
- 자료는 전송도중에 다른 사람에게 보여 지지 말아야 한다(사적비밀).
- 업무를 실행할수 있는 사용자의 신원이 설정되여 있어야 한다(인증).
- 인증된 사용자는 트랜잭션을 실행할수 있는 허가를 가진다(권한부여).

기본적으로 모든 보안요구들이 만족되는것 같지만 문제는 사용자가 이러한 내용을 트랜잭션이 수행되는 대단히 짧은 시간주기에서만 안다는것이다. 일단 트랜잭션이 완성되면 이러한 지식은 없어 지며 다시 설정될수 없다. 왜냐하면 이러한 내용들이 트랜잭션자료와 함께 보관될수 없기때문이다. 그러나 수자식서명은 이러한 지식의 일부를 취하여 보관할수 있게 한다.

수자식서명은 암호화기술과 같은 방법으로 자료를 보호하지 않는다. 수자식서명은 비합법적인 사용자들에게 자료를 숨기지 않는다. 이것은 자료암호화에 의하여 제공된다. 수자식서명은 외부해커 또는 부당한 내부사용자에 의한 자료수정을 막지 못한다. 이러한 문제는 인증과 접근조종에 의하여 제공된다. 수자식서명은 응용프로그람이 보존하려는 자료에 대하여 다음의 두가지 문제를 증명할수 있게 한다.

- **무결성** 자료는 서명된 때부터 수정되지 않는다.
- **원본** 서명자의 신원은 암호기법적으로 증명될수 있다.

응용프로그람자료에 대한 변경을 방지한다는것과 자료가 변경되지 않는다는것을 증명할수 있다는것 사이에는 중요한 차이가 있다. 이것은 그럴듯한것 같지만 사용자가 어

떻게 자기의 접근조종방법이 손상되지 않았다는것을 증명하는가. 보안위반이 일어 나지 않았다는것을 증명하는것보다 보안위반이 일어 났다는것을 증명하는것이 훨씬 더 쉽다. 기관을 속이려는 시도가 탐지된다면 해커는 자기의 목적을 달성할수 없을것이다.

트랜잭션자료가 수자적으로 서명된다면 응용프로그람은 그에 기초하여 자료가 변경되지 않았다는것과 자료접근이 합법적인 사용자에 의하여 진행된다는것을 증명할수 있다. 그러므로 수자식서명이 속임시도를 방지할수는 없지만 응용에 부당한 트랜잭션을 탐지하는 능력을 부여하는 방법으로 속임시도를 성과적으로 방지할수는 있다.

수자식서명 그자체는 이러한 증명을 위하여 응용프로그람과 함께 보관되여야 하는 분리된 자료토막이다. 수자식서명이 응용프로그람의 자료보관요구와 밀착된다는 사실은 왜 수자식서명기능이 다른 보안기능보다 응용프로그람과 더 견고하게 통합되여야 하는가 하는 또 다른 리유로 된다.

콤퓨터에 의한 업무처리

그림 31－2는 수자식서명이 콤퓨터에 의한 업무처리에 어떻게 리용되는가를 보여 준다. 매 단계에서 사용자는 중심자료기지에 보관된 자료를 보거나 수정할수 있는 응용프로그람을 리용하고 있다.

응용프로그람에 의하여 창조되거나 수정되는 문서는 매번 수자식으로 서명된다. 또한 자료는 리용될 때마다 서명이 검증된다. 이것은 사용자가 자료기지에 있는 자료가 진짜이며 합법적인 사용자에 의하여 창조되였다는것을 확신할수 있게 한다. 이것은 또한 보안방책을 강화하며 사용자가 부주의로 이 단계들을 뛰여 넘는것을 방지한다. 응용프로그람이 문서가 언제 서명되며 그것이 언제 검증되는가 그리고 이러한 조작들이 실패한 경우에는 무엇을 해야 하는가를 알아야 하므로 수자식서명은 응용프로그람흐름론리에서 없어서는 안될 하나의 부분으로 되여야 한다.

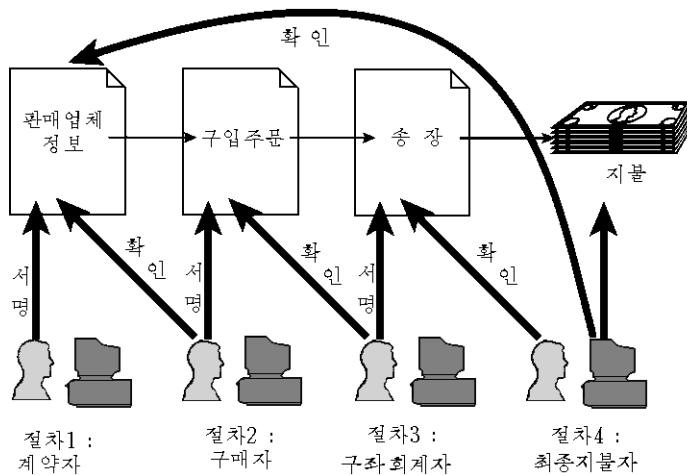



그림 31－2. 전형적인 콤퓨터에 의한 업무처리

자료기지는 각이하다

지금까지 이 장에서는 수자식서명이 왜 다른 보안기술과 차이나는가를 설명하였다. 관계형자료기지응용프로그람은 또한 몇가지 고유한 특징들을 가지고 있다. 그러므로 그에 맞는 수자식서명통합방법을 요구한다.

문서란 무엇인가

수자식으로 서명된 《트랜잭션》에 대해서는 이미 설명하였다. 문서라는 용어도 종종 서명된 자료를 표현하는데 쓰인다(그림 31－3). 수자식서명대안은 매 류형에 따라 문서를 다르게 정의한다. 실례로 전자우편보안제품들은 문서를 전자우편과 그것의 부속물로 정의한다. Word처리문서 또는 계산표(spreadsheet)를 수자식으로 서명하는 보안제품들도 있다. 다른 제품들은 임의의 파일류형을 수자식으로 서명한다. 이러한 문서들이 내부적으로는 명확히 구별되는 많은 자료요소들을 포함하지만 문서는 최종적으로 련속된 바이트렬로 표현된다.

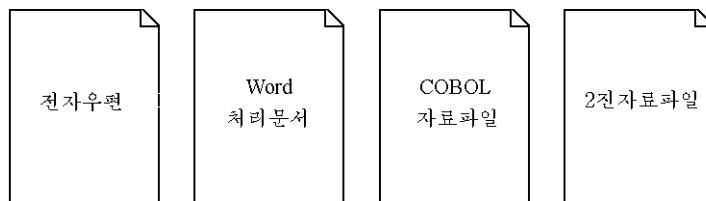



그림 31－3. 문서의 류형

관계형자료기지는 이러한 자료를 완전히 다르게 보관한다. 자료기지는 구조화된 자료를 보관한다. 그러므로 문서를 구성하는 모든 자료요소들은 먼저 류형정의가 되여 있어야 한다. 자료기지는 표준화라는 개념을 리용한다. 이것은 방대한 량의 구조화된 자료를 보관하고 효과적으로 검색할수 있게 한다. 문서에 있는 자료는 표로 기억된다. 표는 행과 렬로 구성된다. 렬은 매 자료명(례컨대 《제품이름》, 《송장번호》, 《주문날자》)과 자료형(례컨대 문자, 수자, 날자)을 정의한다. 레코드라고 부르는 표의 행은 표의 매 렬에 대한 실제자료값을 포함한다.

여기서 《문서》는 관계형자료기지에서 하나이상의 렬과 행으로 구성된 하나이상의 표에 있는 자료로서 정의된다. 즉 문서는 다중자료기지표에서 선택된 하나이상의 렬들과 행들로 구성될수 있다. 그러므로 문서는 대단히 복잡해 질수 있다. 자료기지는 이러한 복잡성을 가지는 방대한 자료를 효과적으로 조정할수 있도록 설계된다.

그림 31－4는 사람들이 인차 알수 있는 규격의 문서를 보여 준다. Gradkell Systems 회사로부터 LLED콤퓨터회사에로의 주문절차는 아주 단순하다. 주문서는 보통 주문번호에 의하여 식별된다. 그림에서는 주문 #123이다. 주문서에는 4개의 항목이 있다. 매 항목

에는 수량, 설명, 가격이 포함된다. 주문서에는 또한 총 가격이 포함된다. 그림 31－5는 주문서가 어떻게 자료기지에 보관되는가를 보여 준다.

주 문 #123

TO : LLED 콤퓨터회사
From : Gradkell Syatem, Inc.
4910 University Place

1	800 Mhz Pentium Ⅲ 처리소자 4개 PowerEdge Server w/Red Hat Linux	$4,750.00
4	512MB PC-100 DIMM 기억기	$250.00
1	SCSI RAID조종기	$1,750.00
3	18GB 10,000 RPM SCSI디스크구동기	$1,250.00

총 가격 : $8,000.00

그림 31－4. 응용프로그람에 의하여 연시 또는 인쇄된 자료기지문서

판매자

판매자코드	이 름	지불주소	. . .
DM	DELL 콤퓨터	1 Dell Way, Round Rock	. . .
PIZ	Dominos Pizza	Down the Street	. . .

주문

주문번호	판매자코드	승인자	총 가격	. . .
123	DM	GGASTON	$25,764.25	. . .
	PIZ	KGASTON	$27.50	. . .

주문항목

주문번호	항목#	량	설명	가격	. . .
123	1	1	4Processor 600 . . .	$4,750.00	. . .
123	2	4	256MB PC-100 DIMM . . .	$250.00	. . .
345	1	2	Large Peperoni+Cheese	$13.75	. . .

강조된 렬들은 주문번호 #123에 속한다

그림 31－5. 자료기지에 기억된 자료기지문서

그림 31－5에 없는 렬들도 그림 31－4에서 연시된다. 이것은 자료기지응용이 내부에서 리용되는 자료만을 포함해야 한다는 리유로서는 중요하다고 볼수 있지만 업무처리에서는 중요하지 않다. 이러한 자료의 실례는 작업흐름에서 문서의 위치를 표시하는 내부기발들이다(례컨대 입력은 되였지만 승인이 되지 않은 경우를 의미한다). 이러한 류형의 자료는 문서의 실제 부분이 아니기때문에 서명할 필요가 없다. 이러한 자료는 처리과정

에 문서이동에만 리용된다. 만일 서명된다면 서명은 자료가 변경될 때 무효로 될것이다. 따라서 전체 레코드를 서명하는것보다는 어느 렬들을 서명에 포함시키는가를 선택하는것이 중요하다.

주문 #123에 포함된 자료는 련속되는 바이트렬이 아니다. 이 자료들은 다른 주문자료(레컨대 번호가 #345인 pizza주문)와 혼합되여 있다. 수자식서명알고리듬은 련속된 바이트렬에 대하여 적용되므로 자료는 자료기지에서 회수되여 련속적인 문자렬형태로 형식화되여야 한다. 또한 이것은 매번 정확히 같은 방법에 의하여 진행되여야 한다. 결과가 같지 않으면 서명이 검증되지 않을것이다. 이것은 수자식서명조작이 자료블로크에 대하여 진행되기때문이다. 암호화가 적용되는 경우에 자료내용은 의미를 가지지 않는다. 서명처리는 오직 자료를 규정된 비트렬로만 본다. 서명검증처리는 단순히 《이것이 서명된 자료인가?》와 《그것이 특정한 사용자에 의하여 서명되였는가?》라는 질문에 대답한다.

자료와 함께 표현되여야 하는 정확도는 어떤 특정한 문제를 제기한다. 자료기지는 수값과 날자값을 특수한 방법으로 보관하며 이러한 값들을 나타내는데 리용되는 가정의 형식을 가지고 있다. 레컨대 날자값이 《1999년 5월 10일 오후 11시 30분》형태로 서명되였지만 《1999–05–10 23:30:00》형태로 검증되였다면 서명은 자료가 변경되였기때문에 검증되지 않는다. 사실 자료표현만이 변경되였지만 그 표현이 자료가 서명될 때와 꼭 같지는 않다. 수값자료의 경우도 마찬가지이다. 실수 47502.5는 《$47,502.50》로 표현될수도 있다. 이것은 수값자료와 날자자료를 표현하기 위하여 자료기지에서 리용되는 기정형식이 자료기지관리자에 의하여 변경될수 있는 경우에 발생하는 문제이다. 이러한 문제들은 자료기지에서 자료가 회복될 때 정확히 자료형식을 규정한다면 해결할수 있다.

통합방법: 왜 응용프로그람통합이 큰 문제로 되는가

보안기능을 응용프로그람에 추가할 때 수자식서명은 다른 보안기술들과 근본적으로 다르다. 그 리유는 다음과 같다.

- 응용프로그람은 업무처리의 적당한 시점에서 문서의 서명과 검증을 교대적으로 적용하여야 한다.
- 응용프로그람은 자료가 서명된 시점에서부터 변경되였다는것이 서명검증에 의하여 밝혀 지는 경우 문서를 거부하든가 또는 처리를 정지시킬수 있어야 한다.
- 수자식서명 그자체는 응용프로그람에 의하여 보관되는 추가정보로서 후에 자료의 무결성과 부인방지를 증명할수 있어야 한다.

정확한 수자식서명처리를 위하여 요구되는 추가적인 응용론리와 자료보관요구들은 수자식서명기능이 보통 완전히 명백한 방법으로 응용프로그람에 추가될수 없다는것을 의미한다.

낮은 준위의 암호화도구를 리용하는 통합

공개열쇠암호화와 PKI는 매우 복잡하다. 암호화알고리듬의 기초에는 현대수학이 동반되여 있으며 암호화는 절대적으로 정확히 실행되여야 한다. 추상구문표기법(ASN.1)과 같이 자료를 부호화하는데 리용되는 자료형식은 매우 복잡하며 낮은 준위의 프로그람작성경험과 함께 ISO와 ANSI표준계렬에 대하여서도 깊은 리해를 가지고 있어야 한다. 증명서고리를 구성하고 확인하는데 필요한 론리를 학습하는것은 매우 어렵다. 다행히 이러한 낮은 준위의 처리를 조종하는 암호화도구들이 존재한다.

그러나 암호화도구를 리용하자면 많은 지식이 필요하다. 개발자들은 수자식서명과 검증에 리용되는 자료구조와 알고리듬에 대하여 완전히 파악하여야 한다. 대부분의 암호화도구들은 개발자들이 C 또는 C++프로그람작성언어를 리용하는것을 전제로 한다. 지어 이러한 도구들을 리용할 때에도 그 내부에서 무엇이 진행되고 있는가를 리해하지 못하면 보안문제에서 재난적인 결과를 초래할수 있다.

보안문제외에도 기관이 응용프로그람보안통합에 이러한 도구들을 리용할 때 제기되는 여러가지 문제들이 있다. 하나의 문제는 높은 위험성이다. 기관들에는 대체로 VB, Power Builder, Oracle Forms, Cold Fusion, JSP, ASP와 같은 개발환경에 익숙한 응용프로그람개발자들은 많지만 C와 C++, PKI프로그람작성, 낮은 준위암호화도구들을 다룰수 있는 개발자들은 적다. 가령 기관에 《체계준위》개발자들이 있다고 하더라도 개발자들이 수자식서명기능을 90%완성한 다음에 기관을 떠난다면 그 다음에는 어떻게 하겠는가. 이 경우에 통합과 유지비용은 높은 비용을 요구하지 않는 제3자의 해결책에 의거하는 비용보다 더 많이 들것이다.

많은 경우에 업무자료기지는 같은 자료에 대하여 여러개의 《전단》을 가진다. 자료는 Web기반응용프로그람으로부터 발생하며 VB로 작성된 응용프로그람에 의하여 내부적으로 처리된다. 흔히 낮은 준위의 도구들을 리용하는 수자식서명통합개발과제는 하나의 응용프로그람 또는 하나의 개발환경으로 제한되여 개발된다. 만일 수자식서명체계가 Web대면부에서만 동작한다면 다른 응용프로그람들에서는 자료가 변경되지 않았다는것을 보증할수 없다.

수자식서명이 내장된 개발환경

낮은 준위의 암호화도구를 리용하는 다른 방법은 수자식서명이 내장된 도구를 리용하여 응용프로그람을 완전히 다시 작성하는것이다. 새로운 체계에서 이것은 아주 잘 동작할수 있다. 실례로 일부 전자문서제품들은 내장된 수자식서명기능을 가지고 있다. 이러한 제품들은 일반종이문서체계를 콤퓨터에 의한 문서체계로 바꾸는데 효과적으로 리용될수 있다. 전자문서는 종이문서와 류사하게 모든 처리를 진행한다. 그러나 서명목적을 위하여 인쇄되지는 말아야 한다. 많은 프로그람묶음들은 관계형자료기지와 통합되여 있다. 그것들은 문서자료의 보관과 회수를 위하여 자료기지를 리용한다. 또한 문서보관을 위하여 자료기지를 리용한다. 그러나 이러한 제품들이 다목적자료기지전단으로 되는것은 아니다. 일부 제품들은 자기자체에 고유한 자료기지구조를 요구한다. 다른 제품들은 기존의

자료기지구조를 통합하는 능력에서 제한성이 있다. 이러한 제품들은 또한 전자문서자체에 자료의 복사본을 보관한다. 그러므로 이러한 제품들을 자료기지전단으로 리용하면 추가적으로 기억과 처리시간이 요구되며 따라서 성능저하가 일어 난다. 보통 전자문서제품들은 자체의 개발환경과 마크로언어를 가지고 있다. 그러므로 수자적으로 서명된 전자문서를 완전히 다시 작성하여 기존의 응용프로그람에 맞게 변환할수 있다.

자료기지접근에 전자문서쏘프트웨어를 리용한다면 전자문서제품을 리용하여 수자식서명을 진행하는것이 좋다. 그것은 수자식서명이 전자문서자체에 보관되기때문이다. 례컨대 자료기지를 리용하는 VB응용프로그람을 작성한다면 수자식서명은 검증될수 없다. 지어 전자문서제품이 수자식서명을 검증할수 있는 프로그람작성대면부를 포함한다고 하여도 전자문서에 보관된 자료복사본을 리용한 검증은 가능하지만 자료기지에 보관된 복사본에 대하여서는 검증이 불가능하다. 이것은 VB응용프로그람이 전자문서에 보관된 자료가 아니라 자료기지에 있는 자료에 기초하여 처리되기때문에 아주 중요한 문제이다. 전자문서서명의 검증은 자료기지에 보관된 자료가 변경된다고 하여도 진행할수 있다.

그러므로 수자식서명기능을 포함한 개발환경을 관계형자료기지에 적용할 때에는 의례히 일부 중요한 제한점들이 존재하게 된다. 이러한 제한은 그러한 개발환경들이 일반목적용자료기지응용개발도구로 설계되지 않은것과 관련된다. 이 개발환경들에서는 흔히 자료기지를 자료의 1차보관매체로 리용하지 않고 선택적으로 또는 보조기능으로 제공한다. 이러한 개발환경에서 수자식서명기능은 다른 류형의 응용에도 리용할수 있도록 설계되지 않는다. 이러한 류형의 수자식서명도구들은 자료중심이 아니라 개발환경중심이다.

관계형자료기지에서 수자식서명의 일반방법

이미 설명한바와 같이 자료기지응용프로그람을 보안하는 현재의 방법은 자료기지봉사기주위에 가상적인 《장벽》을 설치하는것이다. 이러한 장벽에는 망방화벽, 암호화, 강한 인증과 권한부여, 침입탐지 등이 포함된다. 이것은 망보안을 위한 아주 우수한 기능이며 복잡하지만 응용프로그람과는 완전히 독립이다. 그러나 이러한 방법은 자료기지봉사기준위에서 동작하며 트랜잭션(또는 문서)준위에서 자료무결성과 부인방지를 검증하는 기능은 좀 미약하다. 수자식서명은 응용보안에서 다음 단계이다. 그러나 수자식서명기능은 일정한 응용프로그람통합을 요구하기때문에 각이하다. 이 다음 단계에 도달하기 위하여서는 될수록 적은 응용프로그람통합을 요구하는 관계형자료기지에 보관된 자료를 수자식으로 서명하는 응용프로그람과 독립인 체계가 필요하다.

자료기지에 수자식서명을 통합시키는데서 나서는 기초요구

이 장의 다음 부분들에서는 일반자료기지서명체계의 기초설계목적을 설명한다.

응용프로그람개발자들에게 PKI지식이 요구되지 않는다. 응용프로그람개발자들은 수자식서명전문가가 아니라도 된다. 그들은 수자식서명이 무엇인가 하는것도 리해할 필요가

없다. 다만 업무처리과정의 어떤 단계에서 어느 문서에 대하여 어떤 조작이 진행되는가 하는것만은 알아야 한다. 일반자료기지서명체계가 결정할수 없는 응용측면의 5개의 항목들은 다음과 같다.

1. 어떤 류형의 조작이 실행되여야 하는가(례컨대 서명 또는 검증).
2. 어떤 류형의 문서가 서명 또는 검증되는가(례컨대 주문서, 송장, 시간카드, 휴가신청서, 401K참가양식 등).
3. 어떤 특정문서가 서명 또는 검증되는가(례컨대 주열쇠(primary key)는 그 문서를 유일하게 식별하는 값이다).
4. 업무처리의 어느 단계에서 수자식서명 또는 검증이 진행되는가.
5. 서명 또는 검증에서 오유가 발생하면 어떻게 하는가.

이러한 항목들은 응용프로그람개발자들이 알아야 할 문제로서 응용프로그람의 다른 조작들에서 요구되는 정보들과 류사하다. 실례로 응용개발자는 《주문번호 123은 사용자가 sumit단추를 누를 때 서명할 필요가 있다》는것을 알아야 한다. 물론 실제의 처리는 더 복잡하지만 응용프로그람개발자는 표의 어느 렬이 서명되고 서명자료가 어디에 보관되는가 하는 구체적인 세부는 알 필요가 없다.

기존자료기지구조에 대한 수정이 요구되지 않는다 수자식서명체계가 독립적응용프로그람이 되려면 그 어떤 응용프로그람의 자료기지구조에 직접 의존하지 말아야 한다. 그러나 새로운 표를 추가하는것은 문제로 되지 말아야 한다.

서명되는 자료는 지적될수 있다 자료기지가 자료를 련속적인 바이트렬로 보관하지 않기때문에 문서 또는 트랜잭션을 포함하는 자료항목들은 자료기지로부터 수집되여야 한다. 서명된 자료는 그것이 검증될 때 서명되였을때와 꼭 같아야 한다. 이러한 체계는 간단히 통합시킬수 있으며 응용프로그람개발자들에게 있어서 이러한 과제는 단순하다. 그리고 수자식서명이 자료수집단계를 실행하기때문에 자료(표 또는 렬)는 지적될수 있어야 한다. 이러한 지적사항에는 매 자료항목들이 어떻게 형식화되는가(례컨대 《오후 1:00》 또는 《13:00》)를 정의하는 정보가 있어야 한다. 또한 문서의 주열쇠와 기존표들을 서로 련관시키는 합성방법이 있어야 한다.

규모조절할수 있고 단일고장점이 없다 자료기지봉사기와 응용프로그람봉사기는 모두 응용프로그람을 위하여 요구된다. PKI는 등록부봉사기를 추가한다. 수자식서명체계는 봉사기들에서 병목현상 또는 응용프로그람처리정지를 일으키지 말아야 한다.

추가적인 서명보관고는 될수록 작아야 한다 자료기지환경은 자료의 효과적인 보관을 제공할 때에만 우점을 발휘할수 있다. 수자식서명보관의 사실상의 표준은 암호화통보문구문표준인 PKCS #7이다. 이 표준은 서명된 문서와 같은 암호화통보문의 자료구조를 정의한다.

대부분의 마당들은 선택적이지만 표준서명자료통보문에는 서명자의 인증서, 《사슬》구조로 된 다른 CA인증서, 서명된 자료의 복사본이 포함된다. 자료통보문을 서명한 PKCS #7은 《비표준화》된 큰 2진자료토막이다. 자료기지는 서명자와 검증자가 공유하는 중심자료보관고이므로 인증서와 자료를 서명된 매 문서에 보관할 필요는 없다. 이 자

료는 자료기지에 보관되여 있기때문에 《표준화》될수 있다. 인증서는 오직 한번만 보관되고 자료기지관계를 통하여 서명된 문서들과 련결된다. 하나의 인증서는 대략 600~1,000byte이다. PKCS #7통보문은 보통 3개정도의 인증서를 포함한다. 불확정길이를 가진 자료토막은 또한 PKCS #7통보문에서 제거될수 있다. 왜냐하면 자료는 이미 자료기지에 보관되여 있으므로 다시 보관할 필요가 없기때문이다. 그림 31-6에서 보여 준바와 같이 서명정보의 표준화는 수자식서명체계에 요구되는 추가적인 서명기억자료량을 크게 감소시켰다.

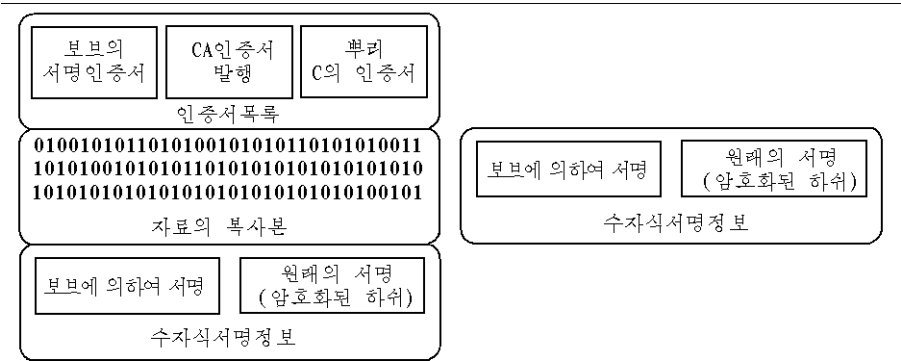



그림 31-6. PKCS #7의 서명된 자료통보문은 자료기지보관을 위하여 최적화된다.

최적화된 PKCS #7은 대략 300byte이다. 자료길이를 1,024byte로 가정할 때 최적화하지 않은 PKCS #7은 3,000byte이상이다. 매 문서에 필요한 자료를 줄임으로써 체계성능을 개선할수 있다. 왜냐하면 망접속을 통한 자료전송량이 줄어 들기때문이다.

수자식서명처리의 추상화

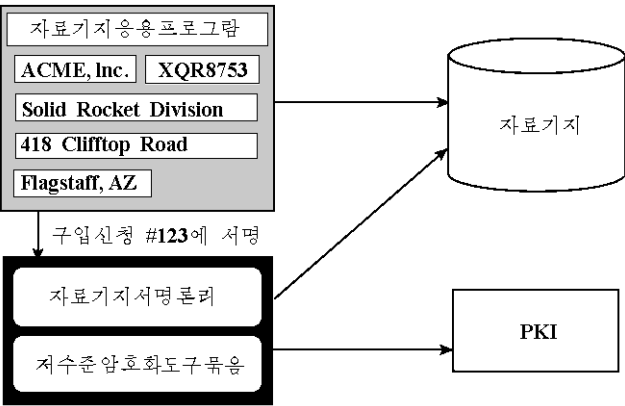



그림 31-7. 자료기지《문서》를 서명하는 공정은
표준화되여 응용프로그람론리로부터 갈라진다

수자식서명통합은 수자식서명기능을 기존의 응용프로그람에 《접착》시킨것으로 볼 수 있다. 실제의 암호화조작과 PKI요소와의 호상작용은 낮은 준위의 암호화도구에 의하여 수행된다. 여기서 《접착제》는 자료기지와 암호화도구가 어떻게 호상작용하는가를 지적하는 프로그람서고이다.

그림 31－7에서 암호화도구는 원래의 자료에 대한 서명처리를 진행한다. 자료기지에서 자료의 수집과 서명정보의 자료기지보관은 자료기지서명론리에서 진행된다. 자료기지서명론리는 자료기지에서 주문요구자료의 회수, 자료서명을 위한 암호화도구의 리용을 조종한다. 또한 관계형자료기지환경에 최적인 보관형식으로 서명자료를 형식화한다.

자료기지에서 수자식서명자료처리는 응용프로그람에 맞게 표준화되고 추상화된다. 그리하여 응용프로그람개발자들은 수자식서명에 대한 구체적인 내용파악이 없이 관련프로그람을 개발할수 있다. 수자식서명과 관련한 처리들은 체계 또는 도구에 의하여 자동적으로 조종된다.

요 약

이 장에서는 수자식서명과 관계형자료기지에서 특징적인 일부 문제들을 설명하였다. 수자식서명은 서명검증을 위하여 보관되는 여러가지 자료형식이므로 각이한 방식으로 진행된다. 관계형자료기지는 또한 특수한 방식으로 자료를 보관하기때문에 각이한 형태로 존재한다. 이 두 차이점들이 호상 합쳐 지면 수자식서명을 관계형자료기지에 결합시키는 것이 복잡하고 지루한 작업으로 되게 된다. 이 중요한 통합단계의 비용과 위험은 많은 응용에서 수자식서명의 리용을 방해하였다. 지금까지 자료기지환경을 위하여 특별히 설계된 수자식서명제품은 없었다. Gradkell Systems회사의 DBsign과 같은 제품들은 수자식서명보안을 관계형자료기지응용에 아주 단순하게 통합시킬수 있게 하고 있다. 이러한 제품들은 특별히 양성된 제3의 개발자들의 암호화 및 보안관련전문지식에 영향을 주어 복잡한 고도기술을 요구하는 통합개발과제를 기관안에서 처리할 때 제기되는 비용과 위험을 훨씬 줄인다. DBsign 또는 Gradkell Systems에 대한 더 자세한 정보는 Web싸이트 www.gradkell.com에서 얻을수 있다.

제３２장. 자료보관고의 보안과 사적비밀

데이비드 본웰
카렌 깁스
애드리언 웰드휘슨

어떻게 개인정보가 상업기관들에 의하여 수집되고 리용되며 분배되는가 하는데 대하여 공동의 관심이 늘어 나고 있고 끊임없이 변하는 오늘의 환경에서 회사들은 소비자들과 관련한 보안과 사적비밀문제를 어떻게 다룰것인가. 소비자들은 자기의 개인정보가 어떻게 리용되는가를 정의하고 결심하는데 습관되여 가기때문에 그들은 모든 형태의 거래에 대하여 자기들의 정보가 사적비밀로 보존되기를 기대할것이다.

사적비밀침해와 관련하여 자료파괴와 개인정보의 해득과 그로부터 오는 실제위협들은 점점 증가하고 있다. 최근의 사건들은 공개적인 대리인들이 보관고자료기지에 대한 자료채취(data mining)기술을 리용하는 기관들에 의한 개인정보침해를 방지할것을 얼마나 요구하고 있는가를 실증해 주고 있다. 유럽동맹은 이미 사적비밀정보를 보호하는 법적문건을 통과시켰다. 류사한 법적문건과 사적비밀정보의 보호를 조정하는 기관들이 오스트랄리아, 카나다, 뉴질랜드, 체스꼬공화국을 비롯한 여러 나라들에 존재하며 많은 나라들이 이에 관심을 돌리기 시작하였다. 정부는 련방통신위원회(FTC)와 련방상업위원회(FTC) 그리고 다른 조정기구들을 발동하여 모든 회사들이 자발적으로 이에 추종하도록 하고 있다.

사적비밀에 대한 우려를 다루는 한가지 전략은 사적비밀정보를 매우 존중하는 건전한 관례와 공정을 개발하고 실행시키는것이다. 그러자면 기업에 필요한 정보수집과 리용을 끊임없이 진행하면서도 규제사항을 준수할수 있는 도구들과 하부구조를 가져야 한다.

이 장에서는 먼저 사적비밀법과 규정, 조절과 관련한 기업문제를 설명한다. 현실적인 기업씨나리오는 소비자별 관점, 민족별관점, 부문별관점, 업계별관점으로부터 전형적인 사적비밀관련업무요구사항들을 제기한다. 각이한 관점들은 체계구조와 기술선택에 영향을 미친다. 이 장에서는 다음으로 각이한 구조적기능의 관점을 통하여 기술적문제들을 설명한다. 장의 요약에서는 보안과 사적비밀요구사항을 자료보관고안에서 그리고 그것을 통하여 기업과 기술구조체계를 어떻게 밀착시키겠는가에 대하여 언급한다.

사적비밀담보를 위한 문제

자료보관고문제는 많은 회사들이 반드시 고려하여야 할 필수적인 전략이다. 오늘날 개인자료를 보호하는 적당한 규칙이 존재하지 않는다면 앞으로 개발되는 기술들은 자료침해와 같은 도전에 부닥칠것이다. 특히 자료보관고의 보안과 사적비밀을 무시하면 이러

한 도전들에 의하여 기관의 자료보관고전략이 침해 당할수 있다.

더우기 여러가지 조절활동이 세계적범위에서 진행되고 있다. 유럽동맹지시 95/46/EC와 97/66/EC가 지금 효력을 나타내고 있으며 유럽동맹안에서도 사적비밀과 관련한 법적문건을 요구하고 있다. 원격통신법령 222분과의 련방통신위원회(FCC)해설서는 소비자소유망정보(CPNI)의 리용을 인정하는 원격통신회사들에 대한 법적요구서를 채택하였다. 나라들사이에서 시민, 기업주, 소비자들의 국경횡단이동이 또한 중요한 사적비밀문제이다.

회사들은 련방무역위원회(FTC), 련방통신위원회(FCC), EU지시, 조절안, 제출안, 다른 림시법안들에 순응할수 있는 능력을 가짐으로써 사적비밀보호에서 주도자로서의 지위를 차지하는데 필요한 대책들을 취하여야 할것이다.

사적비밀보호기능은 기관들에서 다음의 문제들을 해결하는데 도움이 될것이다.

- 어느 자료가 자료보관고에서 개인적으로 식별될수 있는가를 결정한다.
- 개인적인 자료들을 식별하고 수정한다.
- 소비자들이 동의하는 선택(고르기와 제거)을 고려한 자료채취기술을 리용한다.

사적비밀: 기업추동력에 대한 기회와 위협

회사들은 성공을 달성하기 위하여 대부분의 업계들에서 공통인 의견제출을 통하여 기본기업운영을 관리한다. 기업운영과 관련된 두가지 문제는 **소비자획득**과 **소비자보유**이다. 이러한 문제들은 흔히 소비자의 요구를 성실히 만족시켜 주며 소비자봉사를 개선하는 방법으로 이루어 진다. 기업운영의 다른 하나의 문제는 **돈주머니공유**이다. 이 문제는 소비자의 시장부문공유를 늘이기 위한 노력을 통하여 달성된다. 다음의 문제는 **소유총비용**(TCO: total cost of ownership－의뢰기인 개인형콤퓨터나 봉사기 등의 비용뿐만아니라 판본갱신, 유지보수, 사용자양성 등과 같이 도입후에 드는 여러가지 비용을 포함한 콤퓨터체계의 총비용–역주)으로서 업무과정에 지출을 삭감하거나 효과성을 개선하는 과정을 통하여 실현된다.

표 32－1에는 사적비밀과 련관된 모든 업계들에서 기업운영에 영향을 줄수 있는 가능한 기회들과 잠재적인 위협들의 일부를 제시하였다.

소비자의 사적비밀보장은 많은 회사들의 기업상 측면에서 그리고 기술적인 측면에서 일련의 문제들을 제기한다. 기업문제에 대한 1차적인 관심은 기술과 개발결정에 앞서 핵심기업문제를 명백히 해명할수 있게 한다. 그러나 구체적인 고찰을 위하여 사적비밀문제를 여러개의 구성부분으로 분해하는것이 좋다. 사적비밀문제를 기업과 기술적론의로 갈라 놓으면 이 두 분야의 관건적문제들에 주의를 집중할수 있고 문제의 분석에서 잘못된 가정들과 고려하지 못한 문제점들을 찾아 낼수 있다. 사적비밀문제의 기업관점과 기술적관점을 분석하기에 앞서 먼저 사적비밀보안과 비밀성으로 서로 구분할 필요가 있다. 또한 사적비밀방책을 안내하는 규칙들이 서로 다른 기관들에 의하여 제정되였다는것도 정확히 리해하여야 한다. 다음 부분에서 이에 대한 해명을 요점적으로 설명한다.

표 32-1 기업추동력에 대한 기회와 위협

	기 회	위 협
개인정보의 리용	합리적인 리용을 통하여 사회의 신뢰를 높인다.	오용에 대한 사회의 우려 즉 악용에 의하여 초래되는 개별적인 사람들에 대한 비용부담가능성
법과 규정	소비자의 법규정준수에 대한 가능성은 회사의 영상을 개선하고 소송관련비용을 제거하는 경쟁무기로서 쓸모 있다. 즉 핵심기업에 투자를 집중할수 있게 한다	기업에 대한 벌금, 소송, 업무에서의 무능은 운영의 변화나 새로운 하드웨어 및 쏘프트웨어의 구입으로 하여 주권소유자의 가치저락를 초래한다. 즉 핵심기업에 투자를 집중할수 없게 한다.
경제적효과	자료보관고투자는 쓸모 없거나 가치가 적은 자료를 제거함으로써 수집된 자료의 가치를 증대시키고 시장거래비용을 줄이며 소비자수요를 충족시킨다. 즉 정보수집의 가치를 증가시킨다.	위태로운 자료보관고투자는 수집된 정보의 가치를 떨어 뜨리고 정보제거와 관련한 비용을 증가시킨다.

용어해명

사적비밀문제에서 기업과 기술적관점을 리해하기 위하여서는 용어 《사적비밀》(privacy)과 《보안》(security),《비밀성》(confidentiality)의 의미를 리해하는것이 중요하다.

사적비밀은 비법침입의 영향을 받지 않는 개인특권으로 정의된다. 이러한 정의는 많은 나라들에서 효과적으로 리용되고 있으며 많은 자료들에 적용되고 있다.

보안은 정보체계의 속성으로서 특정한 방책상 절차, 정보의 **비밀성**과 **무결성**을 보호하기 위한 담보, 중요한 봉사의 **리용성,** 간접적으로 **사적비밀을** 포괄한다.

비밀성은 정보의 속성을 정의한다. 비밀정보는 기밀정보 또는 민감한 정보, 비법로출되면 해롭거나 편견적인 정보들이다. 보안은 개인정보의 사적비밀과 비밀성담보를 위하여 요구되기때문에 소비자의 사적비밀을 가능하게 하는 해결책으로 되자면 업무과정을 통하여 제출되여야 한다.

그림 32-1은 보안체계내부의 론리흐름을 보여 준다. 이 그림은 공통기준의 사적비밀클라스를 규정한 공통기준 ISO 15408표준에 기초한것이다. 모든 보안서술과 요구들은 일반보안내용에 기초하여 제출한것이다. 이 내용은 《보안은 위협으로부터의 자산보호와 관련된 문제이며 여기서 위협은 보호된 자산을 악용하려는 모든 가능성을 념두에 둔다》라는것을 서술하고 있다. 위협을 방지하기 위하여서는 모든 위협을 고려하여야 한다. 그러나 보안령역에서는 악의 있는 행동 또는 다른 사람의 행동과 관련한 모든 위협들에 대하여서만 깊은 주의가 돌려 진다.

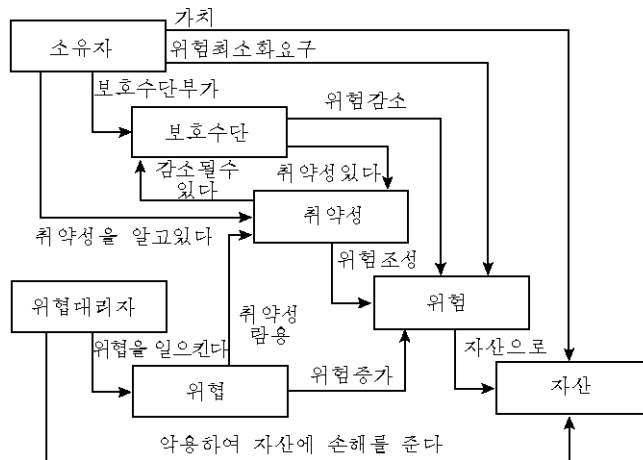



그림 32－1. 보안체계내부의 개념과 관계(론리흐름)

공통기준구조는 론리적인 전진에 따른다. 먼저 보안환경이 서술되고 그 다음 제시된 보안환경에 기초하여 보안목표가 결정된다. 정보보호와 관련한 보안환경의 특징, 보안목표, 보안봉사요구, 보안기능요구에 대한 상세한 설명은 표 32－2에 요점적으로 주었다.

표 32－2 보안요구(ISO 15408)/공동평가기준(CEM)

보안환경

- **전제**: 전제요소의 서술은 소비자환경의 보안측면을 서술하기 위하여 필요하다. 여기에는 물리적인 측면, 직원측면 및 접속측면과 같은 환경리용에 대한 정보뿐아니라 응용의 의도적인 리용, 잠재적인 자산가치, 가능한 리용제한과 관련한 정보들이 포함된다.
- **위협**: 이 요소는 위협인자, 추측되는 공격방법, 있을수 있는 취약성, 보존된 자산식별 등의 용어들로 특징 짓는다.
- **기관의 보안방책**: 이 요소에는 정의된 환경과 관련하여 결정되는 임의의 그리고 모든 법, 기관보안방책과 관례, IT공정들이 포함된다.

보안방책의 위협과 전제만을 고려한다면 기관의 보안방책에 대한 서술을 생략할수도 있다.

보안목표

보안목표는 위협식별, 소비자기관의 방책, 환경전제들을 검토한다. 보안목표를 결정하는 의도는 공학적인 견해, 보안방책, 경제적인자, 위험허용도결정들과 결합된 처리에 기초하여 보안관련문제를 처리하는데 있다.

- **합법적리용**: 정보가 비법사용자에 의해 또는 부당한 방법으로 리용되지 않는다는것을 보증한다.
- **비밀성**: 정보가 비합법적인 사용자에게 로출되거나 제공되지 않는다는것을 보증한다.
- **자료무결성**: 자료의 일관성, 비법적인 창조, 변경, 삭제들의 방지를 보증한다.
- **유효성**: 자료와 봉사가 필요한 경우에 접근가능하다는것을 보증한다.

보안봉사요구

보안목표에 맞게 보안봉사모임 또는 절차들이 요구된다. 보안봉사는 6개의 부분 즉 인증, 접근조종, 비밀성, 무결성, 속성, 리용성으로 나누어 진다.

- **인증**: 사용자 또는 체계가 누구인가를 확인하는 봉사. 인증봉사는 통과암호, 통표, 생체계측정보(례컨대 지문), 암호화 등을 리용하여 진행될수 있다.
- **접근조종**: 사용자, 콤퓨터체계, 공정들이 해당한 권한과 목적에 맞게 자원(파일, 등록부, 콤퓨터, 망)을 리용할수 있게 하는 봉사. 접근조종절차는 신원형접근조종(례컨대 UNIX보호비트, 접근조종목록), 표식형접근조종(즉 위임접근조종) 또는 규칙형접근조종(신원과 표식의 결합 그리고 체계특권에 의하여 실행)으로 수행될수 있다. 접근조종은 비법적리용의 보호와 비밀성 및 무결성보호를 제공하는데서 중요한 역할을 한다.
- **비밀성**: 민감한 개인정보를 비법적인 공개로부터 보존하는 봉사. 비밀성봉사는 모든 암호화를 리용하여 진행된다.
- **무결성**: 자료, 콤퓨터프로그람, 체계자원이 그대로 존재하며 비합법적인 사람, 쏘프트웨어, 콤퓨터환경에 의하여 수정될수 없다는것을 확인하는 봉사. 자료무결성을 보증하는 절차에는 순환여유검사, 검사합, 암호화가 포함된다. 또한 체계무결성을 보증하는 절차에는 물리적인 보호, 비루스방지쏘프트웨어, 보안된 설치절차, 구성조종등이 포함된다.
- **권능**: 체계에 대하여 수행된 작용이 그것을 수행하는 개체에 귀착되며 이러한 작용을 부인하는 개인 또는 체계가 없다는것을 확인하는 봉사. 권능을 제공하는 절차에는 검열, 암호화, 수자식서명이 포함된다.
- **리용성**: 체계, 응용, 자료가 필요한 경우 유용하다는것을 보증하는 봉사. 이를 위하여서는 안전이 요구되는 자료와 중요한 체계봉사들에 해당한 대책을 취함으로써 정확하고 완성된 정보에 기초하여 권한이 부여된 개인들에게 유효한 IT봉사가 진행된다는것을 담보하여야 한다. 임의의 사적비밀보호구조에서 중요한 요구사항은 중요한 자료와 봉사가 언제나 유효하다는것을 보증하는것이다. 유효성을 제공하는 절차에는 고장회복콤퓨터, 비루스방지쏘프트웨어, RAID기억들이 포함된다.

보안기능요구

공동기준 2는 정보의 발견, 비법리용의 보호와 관련하여 4가지 계렬의 용어로 분류한다.

- **닉명**: 닉명은 사용자가 자기의 신원을 밝히지 않고 지원 또는 봉사를 사용할수 있다는것을 보증한다. 닉명은 사용자신원의 보호를 제공하기 위하여 요구된다. 닉명은 인증되여야 하는 신원에 대한 보호는 제공하지 않는다.
- **가명**: 가명은 사용자가 자기의 신원을 밝히지 않고 자원 또는 봉사를 사용하지만 그 리용을 책임질수 있다는것을 보증한다.
- **비련결성**: 사용자는 다중련결에 구애됨이 없이 자원 또는 봉사를 다중사용할수 있다.
- **비관측성**: 사용자는 자원과 봉사가 리용되고 있다는것을 조사할수 있는 제3자와 같은 기타 문제들에 구애됨이 없이 지원 또는 봉사를 사용할수 있다.

이 장의 나머지 부분에서는 회사들이 기업운영에서 산업환경에 맞게 개인적인 정보의 비공개성과 비밀성을 보증하는 보안체계를 실시하고 있다는것을 전제로 한다. 사적비밀에 대한 끊임없는 요구사항으로서의 보안식별을 제외한 다른 문제들은 더 이상 고찰하지 않겠다. 자료보관고에서 보안이 실현되고 사적비밀이 없어 진다는것이 앞으로 언급될수 있다. 그러나 이러한 환경에서도 보안기능이 없이 사적비밀을 가질수는 없다.

규범의 해명

사적비밀방책을 안내하는 규범들은 정부기관, 회사와 시장부문기관, 소비자들을 포함한 각이한 방책들로부터 얻어 진다.

정부규범은 립법기관과 조정기관에 의하여 우선적으로 정의되고 실시되며 정부기구들에 의하여 변경된다. 실례로서 현재 유럽동맹에 의하여 통과된 유럽지시를 들수 있다. 회사와 부문규범은 특정한 시장부문을 구성하는 기업 또는 이러한 시장들과 관계되는 정부기관들에 의하여 정의될수 있다. 실례로서 1995년에 발표된 소비자독점망통신을 조절하는 원격통신개정법안을 들수 있다.

소비자규범은 개인들에 의하여 정의된다. 실례로서 전화하드복사전자우편을 통하여 시장광고를 수신하기 위한 선택안을 들수 있다. 다른 실례는 제3자에게 제공하지 않은 개인자료를 가지기 위한 선택안이다. 개인들이 사적비밀선택안이나 규정을 서술할수 있게 함으로써 매 소비자에 대한 규범의 무결성과 신용성을 유지한다.

기 업 문 제

앞에서 설명한 사적비밀문제는 간단히 다음의 기업문제서술로 요약된다.

> 회사는 개인정보가 어떻게 수집되고 리용되는가를 고려하여 소비자들의 기대와 국내 및 국제법들을 준수하면서 자기 소비자들과 거래할 필요가 있다.

이 장의 다음 부분에서는 기업씨나리오를 조사하여 기업전망으로부터 사적비밀을 가능하게 하는 문제들을 고찰한다. 씨나리오를 시행할 때 발견되는 기업요구사항들은 체계구조와 기술결정을 끌어 내기 위하여 포착되고 리용된다. 사적비밀인식과 민감성에 대한 추가적인 기업요구사항들은 기존법적문건과 대중의 요구로부터 얻어 진다. 사적비밀과 관련한 기업요구사항을 구체적으로 해명하는것은 소비자의 사적비밀을 밀착시킨 구조모형을 창조하는데 도움이 된다.

사적비밀을 담보하는 기업환경

기업씨나리오는 기업환경의 간략서술과 씨나리오에 동반되는 관계자들, 관계자들사이의 거래 등을 포함한다. 그림 32－2는 회사인 경우 소비자의 사적비밀을 보증하는 기

업환경을 보여 준다.

그림 32－2의 왼쪽 부분은 소비자가 회사와 어떻게 어디서 거래하는가 하는 여러가지 선택안들을 보여 준다. 실례는 하드복사전자우편, 전화, 사람, 특수용도의 공중전화팍스, 인터네트를 통한 개인용콤퓨터리용을 보여 주고 있다. 자동결심 또는 지능대리자를 리용한 자동응용과 같은 제3의 거래에 대하여서는 명백히 보여 주지 않았다. 거래는 소비자와 회사사이의 관계를 설정하는 하나이상의 업무(상품과 봉사사이의 실제 교환)로 일어 날수도 있고 그렇지 않을수도 있다.

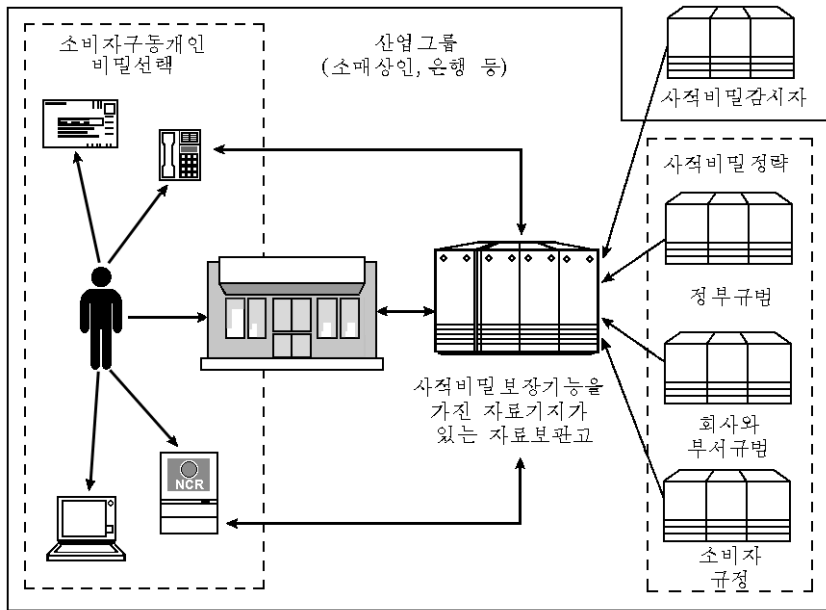



그림 32－2. 소비자사적비밀을 보증하는 기업환경

그림 32－2의 오른쪽 부분은 회사의 사적비밀방책을 끌어 내는 기업규범의 원천을 보여 준다. 소비자의 사적비밀을 보증하는 법적문건의 요구사항은 정부사법권과는 다르다. 또한 소비자사적비밀을 보증하는 산업부문과 회사의 규칙도 다양하게 조정되거나 조종되지 않는 시장과는 다르다. 끝으로 소비자의 사적비밀선택안은 회사의 방책에 따라 통합된다.

그림 32－2의 가운데 부분은 소비자의 개인자료보관싸이트와 함께 회사가 소비자의 사적비밀선택안을 보증하고 실시하는 최적위치 등으로 자료보관고에 대하여 보여 주고 있다.

사적비밀을 가능하게 하는 기업씨나리오

그림 32－3은 이러한 기업씨나리오에 동반되는 기업거래를 시행을 통하여 구체적으로 설명한다. 여기서는 사적비밀방책을 다음과 같이 가정한다.

- 사적비밀방책은 정부, 부문, 소비자의 규칙에 의하여 규정된다.
- 사적비밀방책은 자료기지의 정보구조, 설계, 메타자료봉사와 통합된다.
- 사적비밀방책은 거래의 시작에 앞서 어떤 시점에서 소비자에 의하여 표현된다.

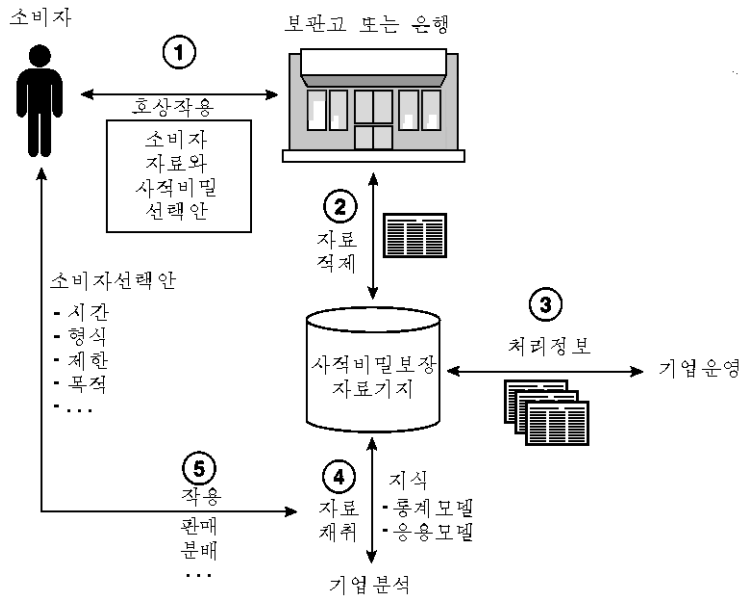



그림 32－3. 소비자의 사적비밀을 가능하게 하는데 동반되는 기업거래

소비자거래

소비자와 업무제공자사이에 협약된 계약은 소비자가 업무제공자와의 업무거래에서 최종적으로 진행되는 거래에 대하여 자발적으로 그리고 빈틈없이 약속될 때 보통 접수된다. 계약은 다음의 동의를 포함한다.

- 업무에 요구되는 개인자료를 보장한다는 소비자의 동의
- 계약리행을 위하여 일정한 기간동안 소비자의 개인자료를 어떤 형식으로 보관하고 리용하며 유지한다는 업무제공자의 동의

소비자는 기업의 신용이 담보되고 서로의 리득 또는 식별의 필요성이 있는 관계에서 추가적인 개인자료(요구되는 목적외에)의 공유를 요구한다. 공유된 자료의 량과 형태는 소비자의 선택안과 기업요구를 명백히 반영하고 포함하여야 한다.

자료적재

기업은 소비자의 거래와 업무를 수집하고 조사하여 무엇이 발생하는가를 반드시 결

정하여야 한다. 이것은 법률, 기업, 통화, 재정, 경쟁 그리고 합법적인 기업기능을 위하여 필요한 다른 측면으로부터 수행될수 있다. 력대적으로 전형적인 보관고소유자들과 은행가들은 자기 소비자들의 움직임과 선택안들을 반드시 기억해 두고 그에 따라 거래를 계속 수정하였다. 그리고 큰 회사들은 자료보관고와 같은 현대적인 도구들의 도움으로 자기의 자료기지에 적재된 지난 시기의 거래와 업무에 대한 수집을 통하여 자기 소비자들의 움직임과 선택안들을 기억하였을것이다.

정보처리

기업이 일단 《무엇이 일어 났는가》를 확정한 다음의 론리적인 단계는 《그것이 왜 일어 났는가》를 알아 내는것이다. 기업들은 거래와 업무에 관한 정보처리에 많은 도구들을 리용한다. 이러한 도구들은 소비자의 움직임과 선택안들을 직관적으로 분석하는데 도움을 준다. 그리하여 최종적으로 회사의 목적과 목표에 맞게 최적방향을 선택하여 더 큰 효과성을 달성할수 있도록 기업운영을 진행할수 있게 한다. 그러나 회사의 간파력이 소비자들의 사적비밀선택안에 따라 서지 못한다면 소비자들은 자기들의 개인자료가 기업의 정보처리에 리용되는것을 환영하지 않을것이다.

자료채취

기업이 《무엇이 일어 났는가》,《그것이 왜 일어 났는가》를 확인한 다음에는 《무엇이 일어 나겠는가》를 예견하기 위하여 자료채취와 분석모형화와 같은 도구와 기술들을 채용한다. 이러한 분석에서는 거래와 업무에 필요한 기업자금과 함께 외부원천으로부터 얻는 가능한 추가정보까지 고려한다. 이때 기업은 이러한 외부정보원천들이 합법적이며 제공하는 정보들이 정확하다는것, 그리고 개인식별자료들이 포함되여 있는 경우에는 소비자들로부터 인정을 받고 있는가를 보증하여야 한다. 분석결과에 얻어 진 예측모형이 소비자레코드에 적용되여 소비자획득, 소비자보유, 소비자증가와 관련한 앞으로의 움직임을 예상한다. 이 모형을 또한 신용, 협잡, 풍족, 다른 기업조건들의 영향을 결정하는데도 리용할수 있다.

행위추적

소비자의 사적비밀을 가능하게 하는 기업씨나리오의 마지막단계는 예측모형결과에 기초하여 실제적인 대책을 취하는것이다. 이러한 대책안들은 법에 위반되거나 소비자의 선택안을 무시하지 말아야 한다. 사적비밀을 고려하는것은 기업움직임에 강한 영향을 미치며 기업운영능력이 떨어 지지 않도록 하면서 사적비밀을 조정하여야 하는 부담, 소비자선택안을 구체적으로 리해하고 반응해야 하는 문제들로 하여 기업운영과 밀접히 련관되여 있다.

요약하면 소비자자료를 조종하고 보관하며 처리하는 기업거래를 통하여 자료를 검사하여 그 변화를 사적비밀이 어떻게 자기 기업안에서 실행될것인가를 결정한다. 법 또는

소비자의 사적비밀선택안에 어긋나게 대책을 취함으로써 기업을 보호하는것은 계약리행이 아니다.

사적비밀담보를 위한 기업요구사항

사적비밀을 보호하는 법적문건개발은 정부의 엄격한 관계와 자체조정방법사이에서 변동한다. 자료보호에 대한 기초원리를 확립한 자발적인 지침이 경제협력개발기구(OECD)의 성원국들에 의하여 1980년에 채택되였다. 이 지침은 개인들에 대하여 수집된 개인관계자료에 관심이 있는 개별적인 시민들의 권리를 인정하고 개인관계자료를 구성하는 파라메터들을 정의하는 법적문건의 채택과 실천을 촉진시켰다.

많은 착상들이 이미 Online Privacy Alliance과 유럽동맹지시기사의 《중요요소》들과 함께 경제협력개발기구(OECD)의 지침에 서술된 사적비밀조항들에 포함되여 사적비밀요구사항에 대한 포괄적인 표로 작성되였다. 이 장에서는 제안된 6개의 사적비밀요구사항들과 련관된 두가지 요구사항들을 요점적으로 개괄한다. 이러한 요구사항들은 체계구조에 적용될 때 매 체계에 대한 사적비밀조정의 영향을 결정하는데 도움이 된다.

사적비밀과 관련한 기업요구사항에는 통지, 선택/동의, 접근, 보안, 제한, 회계가능성, 추적가능성, 닉명/가명의 개념들이 포함된다.

통지 회사는 자기의 소비자들에게 개인자료가 수집되며 어떠한 자료가 수집되는가 그리고 이러한 자료가 어떻게 리용되며 어떻게 발표되는가 하는것을 그들이 쉽게 리해할수 있도록 통지를 제공할수 있어야 한다. 통지서에는 자료수집자와 의도하는 다른 자료수신자의 신원, 자동처리에 동반되는 론리에 대한 정보들이 포함된다.

선택/동의 회사들은 자기의 소비자들에게 특정한 개인자료항목의 선택 또는 제거를 할수 있는 합리적인 선택기능을 제공할수 있어야 한다. 이러한 자료들은 회사의 기업운영에서 사법권과 산업환경요구에 맞게 수집되고 리용되며 발표되여야 한다.

접근 회사들은 자기들이 수집하고 리용하며 발표하는 개인자료들이 정확하며 최신의것이라는것을 자기의 소비자들에게 보증할수 있어야 한다. 접근성에는 개인들이 부정확하거나 또는 불충분한 개인자료를 조사하는 수단 그리고 지역법의 규칙에 따라 수집되지 않은 자료에 대한 접근 막기 또는 제한 권한이 포함된다.

보안 회사들은 자기의 소비자들에게 자기들이 수집하고 리용하며 발표하는 개인자료들이 분실되거나 비법접근, 파괴, 변경, 리용, 발표에 대하여 안전하다는것을 보증하여야 한다.

제한 회사들은 개인자료의 수집과 리용이 명백히 규정된 합법적인 목적을 위해서만 진행되며 초기목적의 수행을 위하여 필요한 기간동안만 규정된 형태로 보존된다는것을 자기의 소비자들에게 보증할수 있어야 한다.

회계가능성 회사들은 자기소비자들이 제정된 사적비밀원리와 실천을 위반할 때 그에 대한 해결책을 찾고 교정할수 있도록 어떤 절차를 세울수 있어야 한다. 회계가능성에는 기존법과 조절구제법, 자기의 주제와 관련한 개인자료수집을 계획한 매개 나라에서

사적비밀권한에 대한 통지서 등의 실시에 대한 지원이 포함된다.

추적가능성 회사들은 조정자들에게 모든 거래와 처리들이 추적가능하며 내부평가 또는 제3자에 의한 평가를 허용하는 방법들에 의하여 경과기록된다는것 그리고 론증하는 소비자들이 사적비밀방책에 따른다는것을 보증할수 있어야 한다. 이것은 국가안전보관소 제안에 추종하는 소비자들에게 있어서는 특별히 중요하다.

닉명/가명 회사들은 자기의 소비자들에게 개인자료가 닉명 또는 가명상태로 유지되여 개인들이 선택할수 있으며 후에 개인을 목표로 리용될수 없다는것을 보증할수 있어야 한다.

요구사항을 구조적인 요소로 넘기기

그림 32－2와 그림 32－3에서 조사한 기업환경과 기업씨나리오는 소비자와 회사사이의 관계를 묘사하고 있다. 구조적으로 보면 3개의 요소들이 소비자의 사적비밀을 보증하는데 영향을 주는 기본부분이라는것을 설명하고 있다. 즉 표현 또는 사적비밀요소와 사적비밀을 보증하는 기업론리 그리고 사적비밀자료이다.

사적비밀표현은 소비자거래에서 《창문》으로 봉사하며 소비자와 관리자 그리고 조작장치와 열람기 등을 포함한다. 사적비밀을 보증하는 기업론리에는 기업거래, 업무, 변환, 분석 및 관리 등이 포함된다. 사적비밀자료에는 자료보관고만아니라 응용내부 또는 더 작은 자료기지에 보관된 중간자료보관고에 대한 문의와 검색, 다른 자료관리조작들이 포함된다.

표 32－3 소비자의 사적비밀을 보증하는 기업요구사항을 구조적인 요소로 넘기기

	사적비밀표현	사적비밀을 보증하는 기업론리	사적비밀자료
통지	○	○	
선택	○	○	○
접근		○	○
보안	○	○	○
제안		○	○
회계가능성		○	
추적가능성		○	○
닉명		○	○

표 32－3에서 보는바와 같이 우에서 설명한 8개의 사적비밀과 관련한 기업요구사항들은 이 3개의 구조적인 요소들에 영향을 준다. 표에서 X는 소비자의 사적비밀을 보증하는 요구사항이 구조적인 요소에 대하여 실행된다는것을 표시한다. 실례로 통지요구사항은 사적비밀표현과 기업론리요소에 대하여 실행되며 사적비밀자료요소에 대한 실행은 요

구하지 않는다. 이미 설명한바와 같이 보안은 소비자의 사적비밀보증을 위하여 요구된다. 그러므로 보안은 모든 구조적인 요소들에 대하여 실행되여야 한다.

소비자의 사적비밀을 보증하는 구조모형

기업요구사항을 구조적인 요소로 넘기는것은 기술적인 선택의 평가에 앞서 기업고려사항에 의하여 먼저 실현을 조사할수 있게 한다. 그림 32－4에서 보여 준 구조적인 모형은 이러한 넘기기를 그라프적으로 설명하고 있다.

모형은 사적비밀표현요소를 통하여 각이한 류형의 대면부로 소비자의 기업체계와 거래할수 있는 각이한 류형의 사용자들을 보여 주고 있다. 이러한 사용자들에는 소비자, 조작자와 관리자, 사적비밀검열자가 포함된다. 또한 사용자에는 사람을 대신하여 조작기능을 수행하는 응용과 대리국들도 포함된다. 모형은 또한 기업론리요소에 영향을 주는 사적비밀규칙의 원천들 즉 정부, 산업/부문, 소비자들도 보여 주고 있다. 또한 보안을 위한 요구사항이 어떻게 소비자의 사적비밀을 보증하는데 영향을 주는 모든 업무과정들을 포함하는가 하는것도 설명한다.

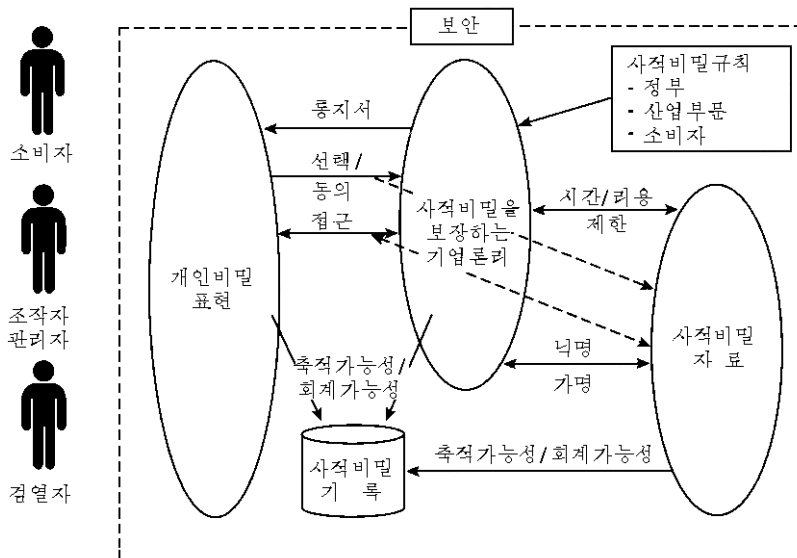



그림 32－4. 소비자의 사적비밀을 보증하는 구조적인 모형

모형은 사적비밀표현과 기업론리요소가 둘다 통지와 자료수집을 동반하는 선택/동의 그리고 자료수집을 동반할수도 있고 동반하지 않을수도 있는 접근과 같은 요구사항들을 처리할수 있는 부분요소들을 포함할 필요가 있다는것을 보여 준다. 또한 시간/리용제한과 닉명/가명과 같은 요구사항들도 기업론리와 사적비밀자료요소가 둘다 포함된 부분요소를 가질 필요가 있다는것을 설명한다.

모형은 앞으로 3개의 모든 구조적요소들의 추적가능성에 대한 요구사항을 취급하기

위하여 부분요소를 포함할 필요가 있다는것을 보여 준다. 이것은 기업에 의하여 정의된 회계가능성절차에 대한 요구사항을 지원하는 경우에도 같이 요구될것이다.

거래할 때 회사들은 사적비밀방책통지서를 보내는 외에 소비자들이 다음의 문제들을 규정할수 있게 하여야 한다.

- 계약된 기업협정범위를 벗어 난 목적에 대하여 추정할수 있는가 없는가.
- 계약된 기업협정범위를 벗어 나 어떤 자료를 공유하려고 하는가.
- 계약된 기업협정범위를 벗어 나 어떤 정황에서 자료를 공유하려 하는가.
- 만일 어떤 자료가 있다면 그것을 보유하려 하는가 또는 팔려고 하는가.

기업을 운영할 때 회사들은 다음의 기능들을 허락할수 있어야 한다.

- 소비자가 자기의 개인자료를 조사할수 있다.
- 소비자가 틀린 자료를 수정할수 있다.
- 소비자가 닉명으로 거래할수 있다.
- 회사가 개인자료보호를 승낙하는가를 조정자가 조사할수 있다.

분석할 때 회사는 다음의 항목들에 따를수 있어야 한다.

- 보유주기에 대한 조정안
- 권한이 있는 리용에 대한 조정안
- 닉명규칙
- 자료보유 또는 판매에 대한 소비자규칙

사람들은 흔히 사적비밀을 조종하는 가장 좋은 위치는 접근시점이라고 생각한다. 그러나 저자들은 사적비밀을 조종하는 가장 좋은 위치는 개인식별정보에 대한 리용규칙이 철저히 실현될수 있는 자료보관고라고 생각한다.

사적비밀을 보증하는데서 요구되는 기능들과 그것을 구조적인 모형에 어떻게 귀착시키는가 하는데 대한 문제들은 이 장의 다음 부분에서 상세히 설명한다.

기술적인 문제

소비자의 사적비밀을 보증하는 기술적인 문제는 현재의 기술에서 소비자의 투자와 기업환경의 급속한 변동, 이미 알려 진 기술, 표준전개 등의 문제로 하여 매우 복잡하다. 기술문제에 대한 다음의 언급은 이러한 우려사항을 보여 준다.

회사들에는 이미 알려 진 사적비밀요구사항을 유지하면서 사적비밀규칙의 변경에 대한

유연성과 성장에 대한 척도화 그리고 성능, 신뢰성, 유효성, 관리가능성에서 접수할수 있는 변경을 제공하는 기술과 봉사가 필요하다.

여기서는 사적비밀을 보증하는 문제를 여러가지 기술적인 관점에서 조사한다. 기업문제를 발견할 때 나타나는 기업요구사항들은 앞으로 이러한 요구사항에 맞추는데 필요한 기능, 처리, 기술들을 식별하기 위하여 구체적으로 조사된다. 기업요구사항들은 기업환경과 함께 구조에 영향을 주는 기술요구사항들의 형식화에 도움을 주는 기술결정을 좌우하게 된다.

사적비밀을 담보하기 위하여 요구되는 기능

표 32－4는 사적비밀을 보증하는 매 기업요구사항을 실현하는데 필요한 자료류형과 함께 기능들을 설명한다. 이 기능들에 적용되는 현재 그리고 이미 알려 진 기술들을 설명한다. 표에서는 이러한 해결을 주장하는 항목들은 밑선으로 표시하였다.

표 32－4 사적비밀보증을 위하여 요구되는 기능

	필요한 기능	필요한 자료류형	기 술
통지	○ 사적비밀방책을 통보한다. ○ 임의의 《자료처리》에 대한 설명을 포함한다. ○ 설비를 추적하는 자료리용(IT체계의 종점사이에서 자료리용을 추적하기 위하여)	○ 회사의 개인비밀보장방책	○ 문서형과 Web기반장치, 규약 ○ 특정한 장치, 공중전화팍스 ○ 스크립트 ○ 메타자료보관고(사적비밀보증자료의 리용을 문서화)
선택/동의	○ 연시되여야 할 특정한 자료요소들을 식별한다. 이러한 요소들은 변경될수 있는데 누구에 의한 변경인가를 식별한다. ○ 개인선택안에 대한 선택항목/현재설정을 표현한다. ○ 개인선택안설정을 만들거나 변경한다. ○ 개인선택안설정을 협상(선택적이다)한다. ○ 개인선택안설정변경을 약속하거나 인정한다.	○ 개인선택안의 선택항목 ○ 개인선택안의 현재설정 ○ 회사의 개인비밀보장방책규정 ○ 사적비밀메타자료 ○ 협상규칙	○ 문서형과 Web기반장치, 규약 ○ 특정한 장치, 공중전화팍스 ○ <u>자료보관고를 동반하는 거래인 경우 사적비밀에 대한 표준은 MDIS이다.</u> ○ <u>자료보관고를 동반하지 않는 거래인 경우 사적비밀에 대한 표준은 P3P이다.</u> ○ 자료를 수집/갱신하는 다매체사용자대면부 ○ 스크립트 ○ 자료기지접근
접근	○ 연시되여야 할 특정한 자료요소들을 식별한다. 이러한 요소들은 변	○ 개인선택안의 현재설정	○ Web기반장치, 규약, 증명절차 ○ 특정한 장치, 공중전화팍스

	경될수 있는데 누구에 의한 변경인가를 식별한다. ○ 요구를 발생하는 사용자에 대하여 ・사용자를 인증한다. ・개인자료를 볼수 있는 접근을 요구한다. ・접근요구에 응답한다. ○ 요구를 발생하는 기업에 대하여 ・현재의 개인선택안설정을 표현한다. ・설정에 대한 갱신을 요구한다. ○ 개인선택안설정을 협약(선택적이다)하거나 변경한다. ○ 특정한 그리고 《허용》된 요소들의 실체를 모두 제거한다. ○ 개인선택안설정변경을 약속하거나 인정한다.	○ 회사의 사적비밀보장방책규칙 ○ 협상규칙	○ 전화쎈터 ○ 문서보고서(OLAP/SQL) ○ 자료보관고를 동반하는 거래인 경우 사적비밀에 대한 표준은 MDIS이다. ○ 자료보관고를 동반하지 않는 거래인 경우 사적비밀에 대한 표준은 P3P이다. ○ 자료수집/갱신하는 다매체/사용자대면부 ○ 스크립트 ○ 자료기지접근(창조, 삭제, 갱신과 삭제) ○ 업무무결성(자료기지갱신의 종합성을 담보하기 위하여)
제한	○ 《리용》제한(회사가 개인자료에 대하여 무엇을 제한할수 있는가)인 경우 리용선택안을 실시한다. ○ 《보유》제한(회사가 얼마동안 개인자료를 리용할수 있으며 얼마동안 알려 지지 않는가)인 경우 보유선택안을 실시한다.	○ 회사의 사적비밀방책규칙 ○ 개인선택안의 현재 설정 ○ 추가로 수집된 자료	○ 《법적문건에 맞는 목적》을 보증하는 응용론리가 실행된다. ○ 기업은 자동처리를 없애기 위하여 수동적이며 자동적인 중재조정을 처리한다. ○ 자료보관고를 동반하는 거래인 경우 《자료기지보기》는 시간/리용제한에 의하여 조종된다. ○ 자료보관고를 동반하지 않는 거래인 경우 보관절차는 시간/제한에 의하여 조종된다. ○ 동적림시변경을 실시하기 위하여 《사적비밀상태정보》개발을 계획한다. ○ 새로운 응용을 보증하는 응용개발기술을 가능하게 하기 위하여 규칙을 고수한다. ○ 합법적리용을 보증하기 위하여 실행환경론리를 적용한다.
회계가능	○ 개인자료의 조종자 또는 처리자인 경우(추적가능성이 요구된다)	○ 회사의 사적비밀보장방책규칙	○ 기업절차 ○ 보안기술(부인방지와 경과기록에

성	·체계에 문의하여 수정한다. ·부인방지능력	○ 개인선택안의 현재설정 ○ 조종자 및 처리자 식별 ○ 사적비밀기록 보관고	대한)
추적가능성	○ 추적가능성을 관리하기 위한 구조와 증명요구사항 ○ 경과기록사건발생, 경고, 례외 등 ○ 경과기록을 조사하고 각이한 자료봉사들사이를 융합시킬수 있는 사용자대면부 ○ 보고서발생 ○ 사적비밀의 고수/승인을 위한 《설비추적》 ○ 경과기록기능을 수행하고 경과기록자료를 보호 ○ 구성조종과 관련한 경과기록을 형성	○ 회사의 사적비밀 보장방책규칙 ○ 개인선택안의 현재설정 ○ 사적비밀기록 보관고	○ 추적가능성을 가능하게 하는 구조선택에 따라 여러가지로 많다. ○ 응용실행환경의 기록(호출경과기록을 준비하고 전송한다).
닉명/가명	○ 닉명(리용에 적용될 때 식별자가 없다). ·개인식별자료를 막거나 떼버리거나 가려 낸다. ○ 가명(자료수집에 식별할수 없는 이름을 배당한다. 그러므로 원천을 찾을수는 있다.) ·적당한 조종을 할수 있는 가명을 발생한다.	○ 리용되는 개인 선택안 설정 ○ 보유하는 개인 선택안설정	○ 자료보관고를 동반하는 거래인 경우 《자료기지》는 닉명으로 조종한다. ○ 자료보관고를 동반하지 않는 거래인 경우 보관절차는 닉명으로 조종한다. ○ 가명발생자

사적비밀을 담보하는 기술전망

기술관점은 기업목표의 초점과 기능 또는 성능과 같은 다른 질적속성들에 의존한다. 각이한 속성들은 각이한 기준에 따르는 기업환경으로부터 특정세부들을 추상화하며 결국 각이한 체계관점이 얻어 진다. 매 관점들은 요소, 호상관계, 지침의 의미에서 독립적으로 정의할수 있다. 그러나 체계의 관점은 독립적이 아니다.

소비자의 사적비밀을 담보하자면 기존구조의 변경이 요구된다. 그러나 완전히 새로운 구조로 변경되는것은 아니다. 다음에 설명하는 기술관점들은 소비자의 사적비밀을 보증하도록 체계구조를 변경시킬 때 고려하여야 할 특정한 측면들만을 포함하고 있다. 이

장의 다음 부분에서는 기능과 성능, 리용성/신뢰성, OA&M(운영, 행정, 관리)관점들을 설명한다.

기능적인 관점 기능적인 관점은 구조모형에서 구별되는 매 요소들의 표현과 통신, 자료흐름, 처리에 대한 구조적인 관점을 제시한다. 구조요소내에서 제시된 기능들은 사적비밀을 보증하는 구조작성블로크들을 포함한다.

사적비밀표현요소 그림 32－5는 소비자의 사적비밀을 보증하는 기업요구사항을 지원하기 위하여 사적비밀표현요소안의 필요한 기능들만을 보여 준다. 5개의 기능적인 구조작성블로크들이 정의된다.

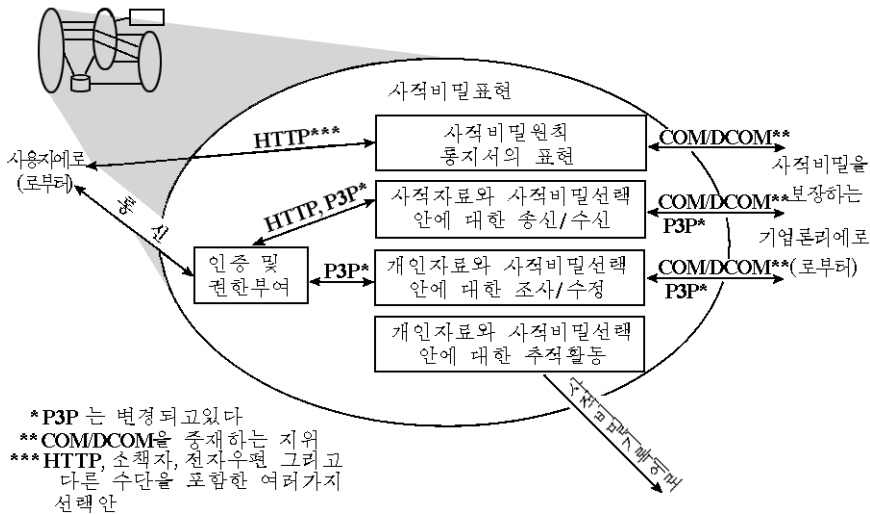



그림 32－5. 소비자의 사적비밀을 보장하는 사적비밀표현요소내에서의 기능들

그림에서 왼쪽에 있는《인증 및 권한부여》블로크는 보안요구사항을 리행하는데 필요한 인증 및 권한부여기능을 나타낸다. 《개인자료와 사적비밀선택안에 대한 추적활동》블로크는 추적가능성과 회계가능성의 요구사항을 리행하는데 필요한 개인자료와 사적비밀선택안에 대하여 수행되는 추적활동기능을 나타낸다. 나머지 3개의 블로크들은 사적비밀보장방책통지서와 선택/동의 그리고 개인자료와 사적비밀선택안의 접근과 관련한 사적비밀요구사항을 리행하는데 필요한 기능들을 나타낸다.

다음으로 사적비밀표현요소를 통한 자료흐름을 설명하자. 초기통신은 어떤 류형의《사용자》(사람, 대리자 또는 다른 응용)와 대방《사용자》대면부사이에 사적비밀표현요소의 실행으로 일어 난다. 이때 사용자에게는 하드복사우편소책자, 전자우편, HTTP 또는 다른 기능을 포함한 여러가지 절차를 통하여 사적비밀보장방책에 대하여 이미 통지되였거나 또는 통지되지 않았을수도 있다. 일단 사용자가 인증되여 사적비밀표현요소에 접근할수 있는 권한을 가지면 사적비밀표현을 포함하여 개인자료를 얻거나 이동, 리용하는 모든 활동은 기록되고 감시된다.

사적비밀표현요소는 사적비밀을 보증하기 위하여 기업론리를 실행하는 요소와《사

용자 》사이에서 개인자료와 사적비밀선택안을 송수신하는 기능을 수행한다. 또한 이 《사용자》가 개인자료와 사적비밀선택안을 조사하고 수정할수 있게 하는 기능도 실행한다. 이러한 조사와 수정은 앞으로는 동적으로 진행되여야 한다. 그러나 현재는 어떤 류형의 문서형보고갱신절차를 통하여 이러한 기능들을 수행하는것이 더 좋을것이다.

자동체계인 경우 사적비밀선택안은 주기적으로 규정되며 소비자들이 기업과 거래할때마다 유지된다. 후자의 경우에 프로그람가능Web대리자는 사적비밀선택안을 규정하고 유지하는 여유처리가 쉽게 되는 절차를 리용하여야 한다. 사적비밀표현기능중에서 통신을 위하여 권고된 표준은 HTTP와 P3P이다(P3P에 대한 Web기반의뢰기의 위치는 제일 많이 변경되였다. 그러나 류형과 사적비밀자료요소를 정의하는 류형과 형식은 다른 조작환경에 맞게 확장되였다).

사적비밀표현기능과 사적비밀을 보증하는 기업론리를 실행하는 기능사이에서 통신을 중재하는 위치는 마이크로쏘프트의 통보문봉사(MSMQ), 마이크로쏘프트의 객체요구매개자의 구조(COM/DCOM) 또는 Web기반봉사(HTTP, P3P)이다. 산업용대면부는 COM/DCOM(DNAf)의 제일 웃준위에 적용된다.

사적비밀을 보증하는 기업론리의 요소 그림 32－6은 소비자의 사적비밀을 보증하는 기업요구사항을 지원하는 기업론리요소내에서 필요한 기능들을 보여 준다. 4개의 기능적인 구조작성블로크가 정의된다. 그림에서 첫 3개의 블로크들은 사적비밀방책의 통지서와 선택/동의 그리고 개인자료와 사적비밀선택안의 접근에 필요한 사적비밀요구사항을 리행하는데 요구되는 기능들을 나타낸다. 특히 이 기능들은 사적비밀방책을 유지하고 기업을 위한 사적비밀규칙을 실시한다. 제일 아래 있는 블로크는 개인자료와 사적비밀선택안에 대하여 수행되는 추적활동기능들을 나타낸다. 이러한 기능들은 추적가능성과 회계가능성의 요구사항을 리행하는데 필요하다.

다음은 사적비밀을 보증하는 기업론리요소를 통하여 자료흐름을 설명한다. 개인자료와 사적비밀선택안을 얻거나 이동하거나 리용하는 모든 활동은 기록되며 감시된다.

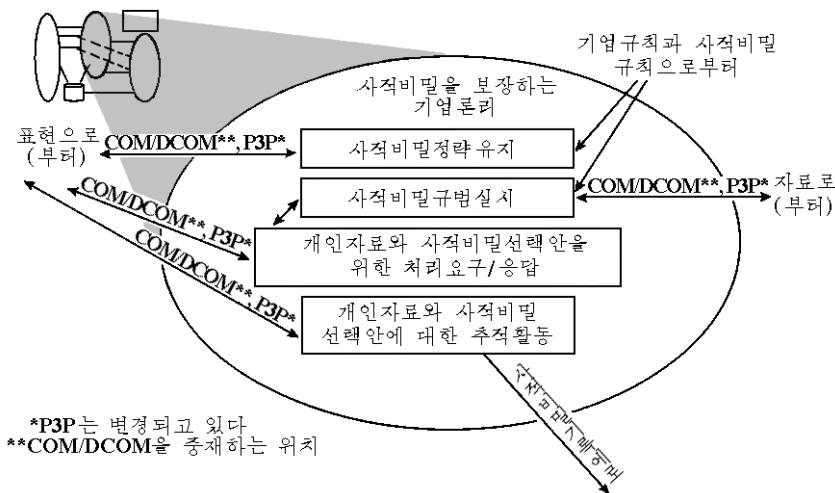



그림 32－6. 소비자의 사적비밀을 보장하는 기업들의 요소내에서의 기능들

기업론리요소는 사적비밀표현과 사적비밀자료요소사이의 개인자료와 사적비밀선택안과 관련한 요구와 응답을 차지하는 기능들을 실행한다. 이러한 요구와 응답을 처리하는 부분으로서 기업론리요소는 또한 기업규칙과 정부, 산업/부문, 소비자의 사적비밀규칙에 관한 원천으로부터 유래되는 사적비밀규칙을 실시하는 기능들도 실행한다.

기업론리기능이 응용내에서 실행될 때 이 기업들의 기능들사이의 통신을 위하여 권고된 표준은 존재하지 않는다. 응용의 조작과 분석을 다루는 기업방책들에서는 정보가 이러한 자동체계내에서 어떻게 통신되는가를 정확히 지적하고 있다.

사적비밀을 보증하는 기업론리를 실행하는 기능과 사적비밀자료기능사이의 통신을 위한 중재위치는 마이크로쏘프트의 객체요구매개자의 구조(COM/DCOM) 또는 Web기반봉사(P3P)이다. 이러한 요소대면부를 통과하는 P3P대화정보는 사적비밀표현요소에서 통과하는 정보와는 다르다. 자료통신에 대한 하부구조(례컨대 특히 CORBA, 통보문화 DB2)는 자기의 하부구조를 적당히 유지하고 있다.

사적비밀자료요소 그림 32－7은 소비자의 사적비밀을 보증하는 기업요구사항을 지원하기 위하여 사적비밀자료요소내에서 필요한 기능들을 보여 준다. 4개의 기능작성블로크가 정의된다.

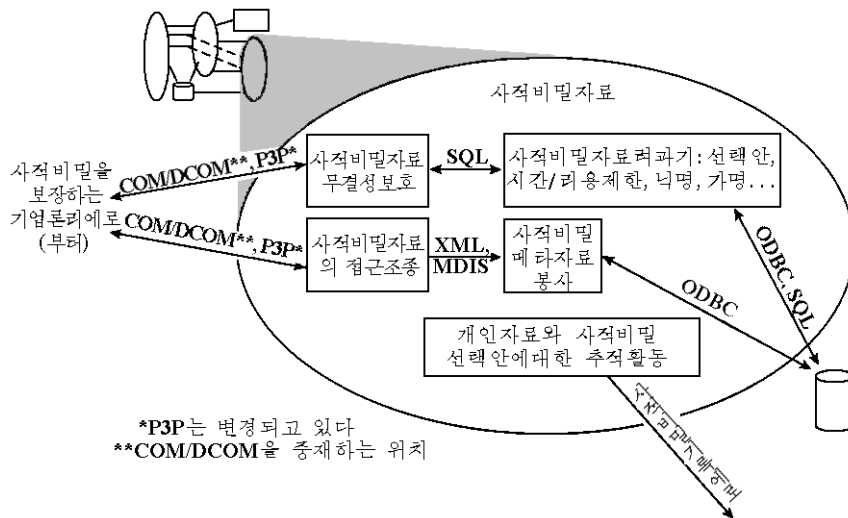



그림 32–7. 소비자의 사적비밀을 보장하는 사적비밀자료요소내에서의 기능들

그림에서 왼쪽에 있는 두 블로크들은 보안요구사항을 리행하는데 필요한 자료무결성보호기능과 자료접근조종기능을 나타낸다. 제일 아래에 있는 블로크는 개인자료와 사적비밀선택안에 대하여 수행되는 추적활동과 관련한 기능들을 나타낸다. 이러한 기능들은 추적가능성과 회계가능성의 요구사항을 리행하는데 필요하다. 나머지 두개의 블로크들은 선택/동의, 개인자료와 사적비밀선택안에 대한 접근, 시간/리용제한, 닉명/가명 등의 사적비밀요구사항을 리행하는데 필요한 기능들을 나타낸다.

사적비밀자료요소는 또한 개인자료접근 또는 기업론리요소에 응답하기전에 이미 형성된 사적비밀선택안에 따라 자료를 려과하는 기능도 수행한다. 더우기 사적비밀자료요

소는 자료기지 또는 특정한 응용프로그람안에 보관된 개인자료에 대한 사적비밀메타자료봉사를 제공하는 기능도 수행한다.

사적비밀자료기능이 비자료기지 응용프로그람에 실행될 때 이 사적비밀자료기능들의 통신에 대하여 권고된 표준안은 존재하지 않는다. 응용의 조작과 분석을 다루는 기업방책들은 자동체내에서 정보들이 어떻게 통신되는가를 정확히 지적하고 있다. 사적비밀자료기능이 자료기지체계 응용안에서 실행될 때 기능들의 통신을 위하여 권고된 표준은 SQL, XML, MDIS, ODBC 그리고 OLE/DB, OLE/DBO이다.

성능관점 성능관점은 소비자의 사적비밀을 보증하는 결과로 구조에 영향을 주는 성능문제들을 다룬다. 임의의 체계에서 성능은 특성 및 기능과 균형을 맞춘다. 균형맞춤은 요구되는 특성과 기능 그리고 접수할수 있는 성능사이에서 이루어 진다.

그림 32－6에서 보여 준 사적비밀표현요소안에서 성능에 크게 영향을 주는 기능들은 선택/동의, 접근(실시간 또는 지연), 추적가능성(경과 기록수준에 따라서), 보안과 관련한 요구사항을 실현하는 기능들이다. 통지를 실현하는 기능들은 성능에 크게 영향을 주지 않을것으로 예상된다.

그림 32－7에서 보여 준 기업론리요소안에서 성능에 크게 영향을 주는 요소들은 선택/동의, 접근(사적비밀규칙의 실시와 관련된), 추적가능성과 관련한 요구사항을 실현하는 기능들이다. 사적비밀규칙의 유지를 실현하는 기능들은 성능에 크게 영향을 주지 않을것으로 예상된다.

그림 32－7에서 보여 준 사적비밀자료요소안에서 성능에 크게 영향을 주는 기능들은 접근, 시간/리용제한, 추적가능성, 보안과 관련한 요구사항을 실현하는 기능들이다. 이와 같이 성능은 개인자료를 어디에 그리고 어떻게 보관하고 유지하는가에 따라 좌우된다. 테라자료보관고를 리용한 실현에서 성능은 영향을 제일 적게 받는다. 왜냐하면 소비자의 사적비밀을 보증하는 요구사항들이 기존자료보관고설계에 적응될수 있기때문이다. 다른 자료보관고, 중간자료보관고, 자료기지류형, 개인자료를 유지하는 다른 류형의 응용프로그람들은 사적비밀요구사항과 관련한 추가기능들로 하여 성능이 일정하게 떨어 진다.

3개의 주요구조요소들사이의 통신실현방법을 어떻게 선택하는가에 따라서도 성능이 좌우된다. 개인의 사적비밀보호(P3P)에 대한 www단체(w3c)의 표준은 여러가지 거래에 대한 성능문제를 내포하고 있다. 그러나 광범한 리용에도 불구하고 이러한 표준이 변경되고 있는 리유로 하여 성능문제가 공개되지 않고 있다.

리용성/신뢰성관점 리용성/신뢰성관점은 소비자의 사적비밀을 보증하기 위한 구조적인 해결의 리용성과 신뢰성에 대한 영향과 관련된다. 리용성은 체계고장사이의 시간과 관련된 문제이고 신뢰성은 체계고장의 주기와 관련된 문제이다. 임의의 체계에서 접수할수 있는 리용성과 신뢰성준위는 산업조작환경의 요구사항에 의하여 결정된다.

매개 산업에서 제기되는 질문은 사적비밀이 체계와 통합되여 사적비밀기록접속과 같은 사적비밀관련요소들이 무효하게 될 때 전체 체계가 정지하는가 안하는가 하는 문제이다. 소비자의 사적비밀과 관련한 세계적인 법적문건이 주어 진다면 대부분의 산업들은 모든 사적비밀관련요소들에 대하여 높은 리용성과 신뢰성을 규정할 필요가 있다. 명백히 규칙이 복잡하면 할수록 실행도 그만큼 복잡해 질것이다.

OA&M관점 OA&M(운영, 행정, 관리)관점은 소비자의 사적비밀을 보증하기 위한 구

조적인 해결의 조작, 주관, 관리에 대한 영향을 취급한다. 임의의 체계에서 OA&M요구사항은 기업방책과 운영환경에 의하여 결정된다. 사적비밀에 의하여 영향을 받는 OA&M체계의 이러한 측면들은 유일하게 구조와만 련관되여 있다.

OA&M체계들은 수단과 하부구조, 관리응용을 실행하는 요소들을 포함한다. 관리하부구조는 전적으로 관리기능을 지원하기 위하여 존재하기때문에 사적비밀요구사항으로부터 일어 나는 이러한 요소들에 대하여 예상되는 영향은 존재하지 않는다. 주되는 영향은 사적비밀을 보증하는 결과에 요구되는 추가적인 수단 그리고 새로운 수단과 관련한 자료를 조종하기 위하여 창조되는 새로운 관리응용들로부터 발생한다.

사적비밀을 위한 수단에 필요한 사건들에는 개인/기밀자료에 대한 접근, 개인/기밀자료요소에 대한 접근주기, 중요한 사건들의 기록, 개인/기밀자료에 대한 여벌복제와 회복, 성능감시 등이 포함된다. 개인자료항목에 대한 발표번호, 위반번호, 경보의 번호와 류형을 설정하기 위하여서는 경계번호가 필요할것이다. 경보는 개인자료에 대한 접근시도뿐아니라 예상하지 못했거나 비법적인 접근시도를 밝혀 내기 위해서도 필요하다.

개인자료를 보관하고 유지하는 어떤 형태의 자료기지를 리용하는 실현인 경우 기존자료관리체계규칙은 사적비밀관련도구프로그람과 사적비밀관련사건들을 감시하는 관리응용프로그람을 확대하기 위하여 필요하다. 합법적인 체계관리자와 자료기지관리자는 사적비밀을 보증하기 위하여 요구되는 추가적인 문제들과 규칙들을 창조하기 위하여 법적문건과 규칙들을 알아야 하며 적응하여야 한다. 이러한 관리자들은 또한 보안을 위하여 사적비밀기록에 대한 배타적인 접근을 가져야 한다.

요 약

이 장에서는 회사들이 자료보관고환경에서 소비자들의 사적비밀과 보안을 보증하는 방향으로 자기의 제품과 봉사를 전개하는데 필요한 문제들을 설명하였다. 회사들은 자기의 산업환경을 시험해 보고 산업구조가 변경되는데 따라 보안과 사적비밀문제를 론의한 이 장의 내용을 리용하기 바란다. 이 장의 내용을 수정하려는 권고안들은 더 합리적이고 더 정확한 정보를 수집하는 과정을 위하여 필요한 문제라고 생각한다.

참 고 문 헌

1. Directive 95/46/EC of the European Parliament and of the Council, 24 October 1995. See also "European Union Directive on Data Protection, Articles" at http://www.odpr.org/restofit/Legislation...les/Directive_Articles.html#anchor3080.
2. Directive 97/66/EC of the European Parliament and of the Council, 15 December 1997.
3. "FTC Releases Report on Consumers' Online Privacy," Report to Congress on Privacy Online, June 4, 1998, http://www.ftc.gov/opa/9806/privacy2.htm.
4. "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," 23 September, 1980. http://www.oecd.org/dsti/sti/secur/prod/PRIV-EN.htm.
5. Privacy Class of Common Criteria v2.0 (CC2.0 part 2) Security Functional Requirements (ISO/ IEC 15408).

제5편
암 호 기 법

암호기법은 해당한 수신자외에는 누구도 그 내용을 읽을수 없게 극비로 써넣는 기술이다. 비밀이나 신뢰성을 목적으로 정보를 변환하는 능력은 쓰기자체의 발생과 함께 존재하여 왔다. 오늘 암호기법의 일부 요소기술들이 접근조종, 인증, 통보문무결성, 부인방지의 실현 등 여러 분야에서 신중한 정보의 보안에 영향을 준다.

쥴리어스 케자르시대에는 자모대입방법을 리용하여 은서법이 나왔다. 실례로 자모글자들을 뒤섞어 놓음으로써 읽기 쉽던 통신문이 뒤범벅이 되고 해독하기 어려워 졌다. 시간이 감에 따라 기존암호화방법론들이 약화되거나 파멸되자 통신문들의 안전성을 보장할수 있도록 점점 더 복잡한 방법론들이 많이 개발되였다.

이 편에서는 암호화기술에 대하여 여러가지로 고찰한다. 제33장에서는 1970년대 초에 개발된 자료암호화표준인 DES의 교체과정을 언급한다. 1997년에 선진암호화표준에 대한 조사연구가 국가적으로 진행되여 DES후보자에 대한 다음과 같은 내용의 설명서가 발표되였다.

- 128bit의 블로크암호화를 리용하는 대칭알고리듬
- 128, 192, 256bit크기의 열쇠지원
- 전 세계적범위에서 특허료없이 사용
- 30년간 자료를 보호할수 있을 정도의 보안제공
- 하드웨어 및 쏘프트웨어적으로 쉽게 실현
- 스마트카드나 이동전화와 같은 환경에서 실현가능

1998년 15개의 AES후보안들이 확정되였으나 1999년에 다시 선택한 결과 그가운데서 다섯개의 대안들이 확정되였다. 2000년 말에 린댈(Rijndael)알고리듬이 당선되였다. 이 글을 쓸 당시는 AES FIPS(Federal Information Processing Standard)의 평가기간인데 최종결말은 2001년 4.4분기에 있게 된다. 이 편의 첫 장에서는 린댈알고리듬의 선택동기, 그것의 견고성, 취약성 등을 비롯하여 상세하게 고찰한다.

이 편의 두번째 장에서는 공개열쇠기반과 단일뿌리열쇠고유의 약점들을 조사한다. 저자는 암호기법적으로 안전한 수자식시간도장의 개념을 소개하면서 PKI내의 그 수자식인증서들은 정확히 설정되면 뿌리열쇠의 가능한 타개로부터 보호된다고 주장한다.

제３３장. 선진암호화표준(AES)에 대한 고찰

벤 로드케

1970년대 초 자료암호화표준(DES: Data Encryption Standard)이 련방정보처리표준(FIPS: Federal Information Processing Standard)으로 되였다. 이것은 거의 소문도 없이 지어 대중적인 관심조차 거의 없이 조용히 일어 난 일이였다. 사실 1960년대 말과 1970년대 초에도 국가적인 암호화시책에 영향을 주고 있던 광범한 대중적관심이 거기에는 전혀 돌려 지지 않고 있었다. 그것은 개인용콤퓨터가 널리 류포되기전에 미리 주의를 돌렸어야 할것이였다. 그때 FIPS의 영향력은 정부가 구매력을 발동할만큼 막강한것이였다. 오늘날에 와서 FIPS의 세력이 소비자시장의 영향을 받는 콤퓨터회사들의 수익성에 미치는 영향은 훨씬 더 적은것이다.

1990년대 말에 이르러 정세는 아주 달라 졌다. DES의 후보로 선출된 선진암호화표준(AES)은 *U. S. Federal Register*와 연구잡지들뿐아니라 소비자콤퓨터잡지들과 주요매체들에까지 선전광고되였다.

AES선출과정은 본질에 있어서 전 세계적으로 론의되고 있는 문제였다. 이것은 세계적으로 제출되는 암호전문가들의 제출안들을 보면 잘 알수 있다. AES과정이 완전히 개방되여 대중적인 여론조사와 론평회들이 진행되였다. 이것은 아주 중요하다. 그것은 효과적인 암호화알고리듬설계에 관하여 력사는 안전한 암호화알고리듬이 허공에서는 설계될수도, 검사될수도, 검증될수도 없다는것을 몇번이나 보여 주었기때문이다. 사실 쏘프트웨어판매업체들이 전용암호화알고리듬을 사용하기로 결정한다면 그것은 곧 그 암호화알고리듬의 안전성과 효과성에 대한 의심을 낳게 될것이다. 조심성에 사로 잡혀 있는 암호화기술의 소비자들은 전용암호화알고리듬을 결코 사용하지 않을것이다.

이 견해는 커크호프(Kerckhoff)의 가설에 기초한것이다. 이 가설에 의하면 암호화체계의 안전은 전적으로 열쇠의 비밀에 달려 있는것이지 알고리듬의 비밀에 따르는것이 아니라는것이다. 그러나 력사는 아직도 일부 판매업체들이 완전히 공개된 암호화알고리듬만이 실지로 세계적수준의 암호화알고리듬으로 설계될수 있는 유일한 길이라는 사실을 망각하고 있다는것을 보여 주고 있다.

AES 과 정

1997년 1월 국가표준화 및 기술연구소(NIST: National Institute of Standards and Technology)(상무성의 한 부서)는 AES과정에 착수하였다. DES의 허점이 늘어 남에 따라 DES의 후보안이 요구되였다. DES에서는 어떤 의의 있는 구조적부분도 찾아 볼수 없었으며 오히려 무어(Moore)의 법칙을 통하여 DES의 약점들이 늘어 났다. 1998년에 들어 와서 적당한 투자결과 DES암호해득장치를 만들수 있게 되였다.

그때까지 DES가 세계적으로 가장 널리 보급되였고 일반목적의 암호화체계였으므로 적수가 DES암호해득장치를 사용할수 있다는것이 가지는 의의가 납득될리 만무하였다.

이 DES암호해득장치의 세부에 대하여서는 Electronic Frontier Foundation에서 출판한 *Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design* (1998. O’Reilly & Assoc., ISBN: 1565925203)을 참고하기 바란다.

DES는 혁신적으로 재설계되여 Triple–DES의 사용을 통하여 정상상태를 회복하였다. Triple–DES는 입력자료를 취하고 그 입력자료를 세번 암호화한다. Triple–DES(ANSI X9.52–1998로 리용되는 공식표준)는 강제적인 공격들에 대하여 유연하며 보안적견지에서도 그만하면 충분하였다. 그러면 왜 새로운 AES로서 간단하게 Triple–DES를 쓰지 않는가. 그것은 DES는 장치적으로 실현할수 있도록 설계되였으며 따라서 쏘프트웨어적실현에서는 효과가 없기때문이였다. Triple–DES는 DES보다 속도가 세배나 뜨다. DES속도가 충분히 빠르다면 Triple–DES의 속도는 너무 느리다. AES에 대한 기준의 하나가 쏘프트웨어적으로 실현될 때 효과가 있어야 한다는것이며 Triple–DES의 기초적인 구성방식은 AES후보자로서는 적합치 못하였다.

AES기술설명서에서는 열쇠의 크기를 128, 192, 256bit까지 지원하면서 128bit크기의 블로크암호화를 리용하는 대칭알고리듬(암호화와 복호화에 같은 열쇠리용)을 요구하였다. 알고리듬은 특허료 없이 전 세계적범위에서 사용되며 30년동안 자료를 보호할수 있는 충분한 수준의 보안을 제공할수 있어야 하였다. 또한 장치적으로는 물론 쏘프트웨어적으로 그리고 제한된 환경들(실례로 스마트카드, DSP, 이동전화, FPGA, 주문ASIC, 위성 등)에서 쉽게 실현할수 있어야 한다.

AES는 정부기관들에서 신중한 안전성을 요하지만 비밀이 아닌 자료들에 리용될것이다. 분명히 모든 징조로 보아 AES는 머지 않아 응당 사영부분에서도 상업거래를 위한 실제상의 암호화표준으로 될것이다.

1998년 8월 NIST는 캘리포니아에서 열린 제1차 AES후보안선출대회에서 15개의 예비적인 AES후보안들을 선출하였다. 그때 15개의 AES후보안들은 전세계적인 암호화사회에서 더욱 강력한 여론조사와 검토를 받았다. 그 과정에는 국가안전보장국(NSA: National Security Agency)도 참여하였다.

여기에서 AES선출과정에 NSA가 참여한 상세한 내용은 언급하지 않지만 NIST가 DES의 발전에 대한 NSA의 교훈을 많이 참작하였다는것을 명백히 해둔다. DES에 대한 초기의 불만은 IBM이 정부의 요청에 따라 DES의 설계원칙들을 비밀에 붙였다는것이다. 이것은 DES가 국가적인 정보사회에 모든 암호화된 자료에로의 완전한 접근을 제공해 주는 어떤 부류의 함정통로를 내포하고 있다는 추측을 낳게 하였다. 그러나 1992년에 DES 설계원칙이 마침내 공개되자 그런 억측은 반박을 당하게 되였다.

AES후보안들

1차 AES후보안선출대회에서 선택된 15개의 AES후보안들을 표 33－1에 렬거하였다.

2차 AES후보안선출대회가 1999년 3월 로마에서 열렸는데 여기서는 1차후보안알고리듬들에 대한 분석검토가 진행되였다. 이 여론조사기간후에 1999년 8월 NIST는 보다 넓은 규모에서 분석검토된 5개의 알고리듬들을 선출하였다(표 33－2 참고).

표 33-1　　　　1차 AES후보안선출대회에서 선택된 AES후보안

알고리듬	제 출 자	요 약
CAST–256	Entrust Technologies, (카나다)	CAST–128과 같은 round함수들을 사용하는 48회불균형 Feistel의 암호. + －XOR회전과 4개의 고정된 6bit S상자를 사용. 하나의 열쇠스케듈지원
Crypton	Future System, Inc.,	&｜XOR회전과 2개의 고정된 8bit S상자들을 사용하는 round함수를 가지는 12회 반복암호. 여러가지 열쇠길이 지원, 이전의 SQUARE암호에서 유래
DEAL	Richard Outerbridge(영국) 와 Lars Knudsen(노르웨이)	약간 차이가 있는 제안인데 round함수로서 현존 DES를 사용하는 6～ 8회 Feistel 암호. 따라서 현존분석들이 많이 리용될수 있지만 속도에서 일정하게 손해를 볼수 있다.
DFC	Centre National pour la Recherche scientifique (프랑스)	상관성기술에 기초하여 설계되고 +×와 round함수에서의 치환을 리용하는 8회 Feistel 암호. 4회열쇠스케듈
E2	Nippon Telegraph 와 Telephone Corporation (일본)	12회 Feistel암호. 하나의 고정된 8bit S상자, 치환, XOR, 혼합연산, 바이트회전들의 대입으로 이루어 진 비선형함수사용
FROG	TecApro International (남아프리카)	8회암호. 매회에서 4개의 기초연산수행(XOR, 단일고정 8bit S상자를 리용한 대입, 들어 오는 매 바이트당 테블값 교체)
HPC	Rich Schroeppel	8회 Feistel암호. +–×&｜XOR회전과 색인테블을 리용하여 8개의 내부 64bit변수들뿐아니라 자료도 수정
LOK197	Lawrie Brown, Josef Pieprzyk, Jennifer Seberry (오스트랄리아)	고정된 11bit, 13bit S상자들과 치환 그리고 +XOR결합을 리용하는 두개의 S–P층이 있는 복잡한 round함수 f를 사용하는 16회 Feistel암호. 복잡한 round함수 f를 사용하는 48회의 불균형 Feistel망을 리용하는 256bit열쇠스케듈
Magenta	Deutsche Telekom (도이칠란드)	6～8회 Feistel암호. 하나의 고정된 S상자(GF(2)에 대한 루승법에 기초)를 리용하는 수많은 대입을 사용하는 round함수사용. XOR를 사용하는 열쇠비트들로 호상결합
MARS	IBM, INC.	8+16+8회불균형 Feistel암호로서 다음과 같은 뚜렷한 네단계를 가진다. 열쇠추가 및 8회의 열쇠 없는 앞방향혼합, 8회의 열쇠 있는 앞방향변환, 8회의 열쇠 있는 뒤방향변환, 8회의 열쇠 없는 뒤방향혼합과 열쇠 있는 덜기. round는 ＋–회전 XOR 그리고 두개의 고정된 8bit S상자를 리용한다.
RC6	RSA Laboratories.	20회 반복암호. RC5로부터 발전. 매회에 자료를 혼합하는데 많은 32bit연산(＋–× XOR회전)리용
Rijndeal	Joan Daemen 과 Vincent Rijmen (벨지끄)	10～14회 반복암호. byte대입. 렬밀기, 행혼합, 열쇠추가뿐아니라 초기 및 마지막 회전에 열쇠추가 리용. 이전의 SQUARE암호에서 유래

SAFER+	Cylink. Corp.	8～16회까지 반복암호. 이전의 SAFER에서 유래. ＋× XOR와 2개의 고정된 8bit S상자리용
SERPENT	Ross Anderson(영국), Eli Biham Lars Knudsen(노르웨이)	32회 Feistel암호. 매회에서 XOR와 회전을 리용하는 열쇠혼합, 8개의 열쇠독립 4bit S상자, 선형변환리용
Twofish	Bruce Schneier John Kelsey 등	4개의 열쇠독립 8bit S상자, 행렬변환, 회전을 리용하며 부분적으로 Blowfish암호에 의존하는 16회 Feistel암호

출처: http://www.adfa.edu.au/~lpb/papers/unz99.html

표 33-2 NIST에서 선출된 5개의 알고리듬

알고리듬	주요장점	주요약점
MARS	높은 안전여유도	실현복잡성
RC6	매우 단순하다	32bit처리소자에 특정한 연산을 리용할 때 안전여유도가 낮다
Rijndael	단순하면서도 기교 있게 설계	불충분한 회수
Serpent	높은 안전여유도	복잡한 설계 및 해석, 유치한 성능
Twofish	상당히 성능 높은 안전여유도	복잡한 설계

18달이상 검사와 분석검토를 진행한후 2000년 10월에 NIST는 린댈알고리듬(Rijndael Algorithm)이 AES후보안으로 선출되였다는것을 공포하였다. 흥미있는것은 NIST의 린댈알고리듬선출에 관한 공포가 발표된지 불과 며칠 지나서 벌써 새로운 표준을 지지하는 광고들이 앞을 다투어 나타나게 되였다는것이다.

2001년 2월 NIST는 AES FIPS초안을 공개적인 심의와 평가에 붙여 2001년 5월 29일 끝마쳤다.

그후 2001년 6월부터 8월에 걸쳐 90일간의 평가기간이 있었다. 대략적인 계획에 따르면 표준화과정은 2001년 4.4분기에 완전한 결말을 보게 되리라는것이 기대되는데 그때 AES는 FIPS로 공식화될것이다.

DES는 사멸하였다.

56bit DES가 비효과적이라는것은 명백하며 사실상 그것은 사멸하였다. 1998년에 들어 서면서 어떤 형태의 높은 수준의 보안체계나 신중한 업무보장체계들에 56bit DES를 실현하는 기관이 더는 없게 되였다. 이런 경우 그것은 즉시 Triple–DES나 다른 공개안전알고리듬으로 갱신되여야 한다.

DES는 1981년에 ANSI표준(ANSI X3.92)으로 수락되고 후에 여러개의 전국은행협회재정봉사(X9)표준들에 통합되였지만 Triple–DES로 교체되기 시작하였다.

암호화알고리듬들은 일반적으로 완전히 호환성이 있으므로 암호화알고리듬교체는 비교적 수월하다. 대부분의 하드웨어실현품들은 플라그인들과 각이한 알고리듬으로의 교체를 허용한다. 가장 큰 난점은 수천수만개의 다른 종류의 장치들을 가지고 있는 회사들에 대한 쏘프트웨어를 교체하는 세부계획에 있다. 또한 원격싸이트들과 위성들을 가지고 있는 그런 기관들에 대하여서는 이 문제가 보다 치명적이다.

AES실현제품들은 이미 많은 상업쏘프트웨어보안제품들에서 선택적알고리듬(Triple–DES 등)을 사용할수 있게끔 출현하고 있다. 쏘프트웨어실현제품들은 하드웨어를 설계하고 갱신하는데 드는 시간때문에 항상 하드웨어제품이 나오기전에 나온다. 일반적으로 쏘프트웨어를 갱신하는것은 하드웨어를 교체하고 갱신하는것보다 더 쉬우며 많은 판매업체들은 이미 자기들의 최신설계들에 통합시킨 AES를 가지고 있다.

이미 Triple–DES를 운영하고 있는 그런 기관들에 대하여서는 즉시 AES를 사용하여야 할 불가피한 리유들이 많지는 않다(호환성제외). 회사들의 AES갱신속도는 보다 많은 제품들이 AES가능방식으로 이동함에 따라 더욱 증가할것 같다.

린댈알고리듬

AES후보안인 린댈은 Proton World International의 죠안 대먼(Joan Daemen)박사와 네데를란드의 카톨릭종합대학 전기공학부 박사과정을 마친 연구사인 빈쎈트 리멘(Vincent Rijmen)이 개발하였다. 대먼과 리멘박사들은 암호화사회에 잘 알려 져 있으며 존경을 받고 있다. 린댈(Rijndael)은 SQUARE암호에 뿌리를 두고 있으며 대먼과 리멘에 의하여 설계되였다.

린댈에 대한 세부들은 초기 AES안에 설명되여 있다. 기술적견지에서 린댈은 열쇠크기에 의존하는 여러회대입선형변환망(substitution–linear transformation network)(즉 비Feistel)이다. 린댈열쇠크기와 블로크크기로는 128, 129, 256bit가 될수 있다. 열쇠와 블로크크기는 임의의 크기를 지원하지 않으며 반드시 이 세개중의 하나라야 한다.

린댈은 바이트입구에 바이트출구를 주도록 동작하는 단일S상자를 리용한다. 실현목적에 따라 그것은 256byte의 색인표로 고찰될수 있다. 린댈은 마당GF(2)에 대하여

$$S(x)=M(1/x)+b$$

로 정의되는데 여기서 M은 행렬이고 b는 상수이다.

린댈에 의하여 처리되는 자료블로크는 바이트들의 묶음으로 분할되며 매 암호연산은 바이트단위로 진행된다. 린댈의 10회암호화에서 매회는 4개의 연산을 수행한다. 첫 계층에서 8×8S상자(비선형구성요소로서 리용되는 S상자들)는 매 바이트에 적용된다. 두번째 계층과 세번째 계층들은 선형혼합계층들인데 거기에서 배렬의 렬들에는 밀기연산이 진행되며 행들에는 혼합연산이 진행된다. 네번째 계층에서 부분열쇠바이트

들에는 배렬의 매 바이트들에로 XOR연산이 진행된다. 마지막회에서 행의 혼합은 생략된다.

NIST는 왜 린댈알고리듬을 선택하였는가

NIST의 언급에 따르면 린댈은 안전성, 성능, 효과성이 결합되고 실현하기 쉬우며 유연성이 있기때문에 선출되였다고 한다.

특히 NIST는 다음과 같은 근거로 하여 린댈이 아주 적합하다고 인정하였다.

- 넓은 범위의 콤퓨터환경에서 하드웨어 및 쏘프트웨어적인 성능이 좋다.
- 귀환 및 비귀환방식에서 다 성능이 좋다.
- 열쇠설정시간상 아주 우수하다.
- 열쇠민첩성이 좋다.
- 매우 적은 기억용량을 요구한다.
- 파워(power)공격과 타이밍(timing)공격에 대처한 방어가 쉽다(이 방어는 힘들게 어떤 처리를 진행하지 않고 보장될수 있다).

린댈의 문제점

일반적인 여론은 린댈이 근본적으로 최상의 알고리듬이라고 하지만 상반되는 견해가 없는것은 아니다. 하나의 문제는 그것의 근저구성방식에 있는바 일부 사람들은 린댈의 수학적기초가 단순하며 그 점에서는 거의 미발육단계라고 의견을 제기하였다. 만일 린댈을 수학식으로 전개한다면 임의의 다른 AES후보안들보다 훨씬 더 간단할것이다. 다른 하나의 비평은 린댈이 적수로부터 자기 암호화기교를 숨기기 위한 혼란기술(obfuscation technique)을 하나도 쓰지 않는다는것이였다. 끝으로 암호화와 복호화연산에 같은 S상자를 리용하는 DES와는 반대로 린댈은 서로 다른 S상자를 리용한다는것이 지적되였다. 이것은 암호화연산과 복호화연산에 서로 다른 S상자를 리용하는 린댈실현이 한번만 연산을 진행하는 실현보다 두배의 품이 들며 속박장치들에 대하여서는 불편할수 있다는것을 의미한다.

린댈팀은 보다 단순한 수학은 린댈을 하드웨어내장제품으로 보다 쉽게 실현할수 있게 한다고 하면서 자기들의 설계를 옹호해 나섰다. 그들은 또한 혼란기술은 필요가 없다고 주장하였다. 이것은 뒤를 이어 린댈팀이 Hitachi로부터의 조사를 모면하기 위하여 혼란기술을 회피하였다는 억측을 낳게 하였다. Hitachi는 자기들의 의향은 자기의 특허들을 위협하는 대상들에 대한 합법적활동을 모색하기 위한데 있다고 표명하였다. Hitachi는 여러가지 암호화혼란기술들에 대한 독점적인 특허들을 유지할것을 주장하고 있는데 그밖의 어떤 다른 단체에 그 기술들에 대한 특허가 넘어 가겠는가 하는것은 아직 미정이다. 사

실 2000년초 Hitachi는 4개의 AES후보안들(MARS, RC6, Serpent, Twofish)에 대하여 특허권청구서들을 제출하였다.

AES를 해득할수 있는가

*Cracking DES: Secrets of Encryption Research, Wiretap Politics & Chip Design*에 상세히 서술된바와 같이 공개DES해득기가 개발되였지만 여전히 AES해득장치가 개발될수 있는가 라는 질문이 존재하고 있다.

DES에 대한 공격은 거의 30년간의 연구후에도 쉽게 발견되지 않았다고 언급되였을것이다. DES에 대하여 유일하게 가능한 공격은 전체 열쇠공간을 무자비하게 빠짐없이 탐색하는것이다. DES의 초기열쇠공간이 증가되였었다면 AES과정은 착수되지 않았을상 싶다.

가능한 모든 열쇠값들을 다 취해 보면서 오랜 시간후에야 DES열쇠를 되찾을수 있는 DES암호해득기들이 제작되였다. AES암호해득기도 역시 나올수 있지만 단일열쇠를 추출해 내는데 요구되는 시간은 상상을 초월할것이다.

실례로 전체 DES열쇠공간은 48시간안에 해득될수 있지만 AES의 경우는 다르다. 만일 FPGA(Field–Programmable Gate Array)와 같은 특별한 목적의 소자가 초당 10억 AES복호화연산을 수행할수 있고 암호해득호스트가 병렬로 동작하는 10억개의 소편을 가지고 있다고 해도 그 열쇠를 되찾는데는 상상할수 없는 시간이 요구될것이다. 만일 DES열쇠를 1초에 해득할수 있는 기계가 개발되였다고 가정한다고 해도 그 기계가 128bit AES열쇠를 해득하는데는 140조년이 걸릴것이다.

AES의 불해득성(적어도 현존콤퓨터와 수학의 능력으로)으로 보아 2030년까지도 안전성의 요구를 충분히 만족시킬것이다. 그러나 다음에는 다시 DES가 언제 처음으로 설계되였는가 하는것을 생각해 본다면…

결론적으로 말하면 실험실적단계로부터 실지 응용단계에로의 량자콤퓨터의 변혁 그 자체를 가정한다면 그것은 AES와 다른 암호화체계에 의하여 제공되는 안전성을 은근히 위협할것이다.

AES에 대한 반응

AES를 제품화에로 추동한것은 정부와 재정봉사회사들이다. 이 두 대상에 대하여 AES의 역할은 아주 다를것이다.

정부측에 대하여 이야기한다면 AES가 FIPS로 확정된후 정부의 모든 기관들은 안전(그러나 비밀은 아닌)체계에 AES를 사용할 필요가 있었다. 정부는 수만대의 체계들에 DES와 Triple–DES를 실현하고 있었기때문에 AES로 갱신하는데 드는 시간과 비용은 막대한것이였다.

AES는 현존 정부시설의 DES, Triple–DES 그리고 다른 암호화체계들을 교체하는데

막대한 시간과 자원의 투자를 요구하였다. AES도입의 지연을 더욱 심화시킨 요인은 Triple–DES가 기본적으로 안전하므로(그의 주되는 우려점은 속도에 있다) 그것을 교체하도록 강요할만한 안전상 긴박성은 제기되지 않는다는 사실이였다. AES가 필요할수는 있지만 정부기관들에 있어서 그것을 실지로 실현하는것과는 반대로 AES도입을 기권하는편이 보다 쉬웠다. AES로 교체하는데 드는 예산과 시간의 압박으로 하여 교체하여야 할 많은 부분들과 실리상 문제들을 안은채로 그 이행과정은 천천히 일어 날것이다.

재정봉사분야에서도 역시 Triple–DES에 막대한 투자를 하고 있다. 재정봉사분야에서는 현재 AES리용에 대한 특별한 요구가 없고 Triple–DES가 우세를 차지하고 있으므로 과연 어느 은행업표준화업체가 AES사용을 요구하겠는가 하는것이 의심스럽다.

DES(X9.23–1955로 암호화됨, Encryption of Wholescale Financial Message)하나만 사용하려는 시도는 X9회의(X9 TG–25–1999를 참고)에 의하여 움츠러 들고 있지만 X9도 역시 다른 알고리듬이 실현될 때까지 DES를 계속 사용하는것을 허락하고 있다.

그러나 AES는 하드웨어 및 쏘프트웨어적인 실현에 효과성이 있고 높은 성능을 가지고 있지만 대규모적인 비정부싸이트의 실현, 갱신에 대한 실리상의 압박초래, Triple–DES의 리용과 결합 등의 어려운 형세를 찾아 볼수 있다. 어차피 이 알고리듬이 전세계적으로 보급되기까지는 많은 시일이 걸릴것 같다.

참 고 문 헌

1. FIPS 46-3, see http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. Reaffirmed for the final time on October 25, 1999.
2. Under the Information Technology Management Reform Act (Public Law 104-106), the Secretary of Commerce approves standards and guidelines that are developed by the National Institute of Standards and Technology (NIST) for federal computer systems. These standards and guidelines are issued by NIST as Federal Information Processing Standards (FIPS) for use governmentwide. NIST develops FIPS when there are compelling federal government requirements, such as for security and interoperability, and there are no acceptable industry standards or solutions.
3. While IBM and the U.S. Government essentially designed DES between them in what was billed as a public process, it attracted very little public interest at the time.
4. See B. Schneier, Security in the Real World: How to Evaluate Security Technology, *Computer Security Journal,* 15(4), 1999; and B. Rothke, Free Lunch, *Information Security Magazine,* Feb. 1999, www.infosecuritymag.com.
5. There are actually six assumptions. Dutch cryptographer Auguste Kerckhoff wrote *La Cryptographie Militare* (Military Cryptography) in 1883. His work set forth six highly desirable elements for encryption systems:
   a. A cipher should be unbreakable. If it cannot be theoretically proven to be unbreakable, it should at least be unbreakable in practice.
   b. If one's adversary knows the method of encipherment, this should not prevent one from continuing to use the cipher.
   c. It should be possible to memorize the key without having to write it down, and it should be easy to change to a different key.
   d. Messages, after being enciphered, should be in a form that can be sent by telegraph.
   e. If a cipher machine, code book, or the like is involved, any such items required should be portable and usable by one person without assistance.
   f. Enciphering or deciphering messages in the system should not cause mental strain, and should not require following a long and complicated procedure.

6. http://csrc.nist.gov/encryption/aes/pre-round1/aes_9701.txt.
7. Details are also available at www.eff.org/descracker.html.
8. The X9.52 standard defines triple-DES encryption with keys k_1, k_2 *and* k_3; k_3 as:
   $C = E_{k3} (D_{k2} (E_{k1} (M)))$
   where E_k and D_k denote DES encryption and DES decryption, respectively, with the key k.
9. It should be noted that AES (like DES) will only be used to protect sensitive, but unclassified data. Classified data is protected by separate, confidential algorithms.
10. Dan Coppersmith, The Data Encryption Standard and Its Strength Against Attacks, IBM Report RC18613.
11. http://csrc.nist.gov/encryption/aes/draftfips/fr-AES-200102.html.
12. For a quick technical overview of Rijnadel, see http://www.baltimore.com/devzone/aes/tech_overview.html.
13. www.esat.kuleuven.ac.be/~rijmen/square/index.html.
14. Available at www.esat.kuleuven.ac.be/~rijmen/rijndael/rijndaeldocV2.zip.
15. http://csrc.nist.gov/encryption/aes/round2/r2report.pdf.
16. Feistel ciphers are block ciphers in which the 2t-bit input is split in half. Feistel ciphers are provably invertible. Decryption is the algorithm in reverse, with subkeys used in the opposite order.
17. Of the four other AES finalists, MARS uses an extended Feistel network; RC6 and Twofish use a standard Feistel networks; and Serpent uses a single substitution-permutation network.
18. Known as the key schedule, the Rijndael key (which is from 128 to 256 bits) is fed into the key schedule. This key schedule is used to generate the sub-keys, which are the keys used for each round. Each sub-key is as long as the block being enciphered, and thus, if 128 bits long, is made up of 16 bytes. A good explanation of the Rijndael key schedule can be found at http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm.
19. http://csrc.nist.gov/encryption/aes.
20. As clarified in the report by NIST (*Report on the Development of the Advanced Encryption Standard*), the fact that NIST rejected MARS, RC6, Serpent, and Twofish does not mean that they were inadequate for independent use. Rather, the sum of all benefits dictated that Rijndael was the best candidate for the AES. The report concludes that "all five algorithms appear to have adequate security for the AES."
21. Improved Cryptanalysis of Rijndael, N. Ferguson, J. Kelsey, et al., www.counterpane.com/rijndael.html.
22. Contrast this with Twofish, see *The Twofish Team's Final Comments on AES Selection*, www.counterpane.com/twofish-final.html.
23. www.planetit.com/techcenters/docs/security/qa/PIT20001106S0015.
24. It is an acceptable assumption to believe that the NSA has had this capability for a long time.
25. An FPGA is an integrated circuit that can be programmed in the field after manufacture. They are heavily used by engineers in the design of specialized integrated circuits that can later be produced in large quantities for distribution to computer manufacturers and end users.
26. Similar to those government agencies that applied for waivers to get out of the requirement for C2 (*Orange Book*) certification.

For Further Information

1. Savard, John, How Does Rijndael Work? www.securityportal.com/articles/rijndael20001012.html and http://home.ecn.ab.ca/~jsavard/crypto/co040801.htm.
2. Tsai, Melvin, AES: An Overview of the Rijndael Encryption Algorithm, www.gigascale.org/mescal/forum/65.html.
3. Landau, Susan, Communications Security for the Twenty-first Century: The Advanced Encryption Standard and Standing the Test of Time: The Data Encryption Standard, www.ams.org/notices/200004/fea-landau.pdf and www.ams.org/notices/200003/fea-landau.pdf.
4. Schneier, Bruce, *Applied Cryptography*, John Wiley & Sons, 1996, ISBN: 0-471-11709-9.
5. Menezes, Alfred, *Handbook of Applied Cryptography*, CRC Press, 1996, ISBN: 0849385237.
6. Anderson, Ross, *Security Engineering*, John Wiley & Sons, 2001, 0-471-38922-6.
7. Brown, Lawrie, *A Current Perspective on Encryption Algorithms*, http://www.adfa.edu.au/~lpb/papers/unz99.html.

제34장. 공개열쇠계층구조의 보호

져프리 씨 그라보우

공개열쇠기반(PKI: Public Key Infrastructure)은 항상 뿌리열쇠라는 웃준위열쇠와 함께 설계되여 왔다. 이 단일열쇠는 계층구조에서 그 단일열쇠 밑에 있는 모든 실체들에 대한 신뢰의 출발점을 보장한다. 만일 이 뿌리열쇠가 타개되기라도 하면 전반적신뢰계층구조는 곧 의문시되게 된다.

뿌리열쇠는 수자식으로 서명하는 하위의 인증국(CA: Certificate Authority)들에 근본적으로 영향을 마친다. 뿌리열쇠의 타개는 사용자에게 비합법적인 CA가 완전히 타당한것처럼 보이게 할것이다. 그러면 사용자는 자기가 믿고 있는 안전성이 터무니 없는것이라는것도 모르고 그 거래에 완전히 말려 들것이다.

단일뿌리열쇠는 단일점고장을 초래한다.

체계의 임의의 부분을 비극적인 고장으로부터 막도록 일련의 억제력과 안정성을 가진 체계로 설계하고 건설하는것은 보안에서 표준적인 실천규범이다. 그러나 모든 실제적인 목적을 실현하는데서 이러한 실천은 계층적인 PKI에 관하여서는 무시되여 왔다.

이 장에서는 이 단일점고장을 제거하는 체계를 제안하는데 목적을 둔다.

암호기법적으로 안전한 수자식시간도장(CSDT: Cryptographically Secure Digital Timestamp)들은 문서보관, 수자식인증 등을 포함하여 여러가지 목적에 리용되여 왔다. CSDT를 PKI내에서 발행되는 모든 수자식인증서들에 추가함으로써 사람들은 현재 그 인증서가 타당한가 하는것은 물론 어떤 점에 타당한가 하는것을 확인할수 있는 방법론을 가질수 있게 되였다.

CSDT를 리용하여 보호되는 PKI내의 인증서들은 알맞게 설정해 놓기만 하면 뿌리열쇠의 타개로부터 구출될수 있다. 만일 뿌리열쇠가 로출된다 하여도 인증서들은 여전히 자기의 초기값을 가지고 있으며 잃는것이란 새로운 인증서를 만들수 있는 능력이 전부이다. 그리하여 거래는 계속될수 있으며 회복공정에는 다만 뿌리열쇠의 교체만이 필요할뿐이다.

여기서 제안된 체계의 주목할만한 우점은 그것이 현존 PKI표준에 설정된 파라메터들안에서 동작한다는것이다.

공개열쇠기반(PKI)

공개열쇠(또는 비대칭)암호기법은 보통 공개열쇠와 비밀열쇠라고 부르는 서로 다른 두개의 열쇠를 리용한다. K_{PUB}(수신자)에 의하여 암호화된 임의의 정보는 오직 K_{PRI}(수신자)에 의하여서만 복호화될수 있으며 반대로 K_{PRI}(수신자)에 의하여 암호화된 임의의 정보는 K_{PUB}(수신자)에 의해서만 복호화될수 있다. 두개의 열쇠들은 수학적으로 련결되며 공개열쇠로부터 비밀열쇠를 결정한다는것은 계산불가능하다. 이로부터 수신자는 하나의

열쇠쌍을 만들고 K_{PUB}(수신자)는 임의의 사람이 다 볼수 있는 위치에 공개할수 있다. 일단 송신자가 K_{PUB}(수신자)의 복사본을 가지면 암호화된 정보는 비밀열쇠를 보낼 필요없이 수신자에게 송신될수 있다.

송신자:

DATA+K_{PUB}(수신자)+암호화알고리듬 = EK_{PUB}(수신자)[자료]

수신자:

EK_{PUB}(수신자)[자료]+K_{PRI}(수신자)+복호화알고리듬 = 자료

이것의 반대과정도 역시 성립한다. 만일 수신자가 자료를 K_{PRI}(수신자)로 암호화하면 그것은 K_{PUB}(수신자)로 복호화될수 있다. 이것은 임의의 사람이 정보를 복호화할수 있고 신뢰성이 담보되지 않았다는것을 의미하지만 자료가 K_{PUB}(수신자)를 리용하여 복호화 될수 있다면 오직 K_{PRI}(수신자)로써만 그것을 암호화했을수 있으며 따라서 그 자료를 보낸 사람을 확인할수 있을것이다. 이것이 바로 수자식서명의 배경에 놓인 원리이다. 그러나 실제 수자식서명체계에서는 처리시간을 절약하기 위하여 오직 자료의 하쉬만을 암호화/복호화한다.

표준PKI계층구조

비대칭열쇠체계들은 전통적대칭열쇠체계들이 안고 있던 열쇠관리문제를 해결하였지만 《관리신뢰성》이라는 새로운 문제를 초래하였다. 이 문제는 《내가 리용하고 있는 공개열쇠가 해당수신자의것이라고 어떻게 장담하겠는가?》라는 질문을 낳게 한다. 전형적으로 제3자공격(man–in–the–middle attack)이라고 부르는 이 문제는 제3자(공격자)가 자기의 공개열쇠를 송신자에게 보낼 때 발생하게 되는데 송신자는 어리석게도 그것이 수신자의 공개열쇠인것으로 믿으며 반대로 공격자가 자기의 공개열쇠를 수신자에게 보내면 수신자는 그것을 송신자의 공개열쇠인것으로 믿게 된다. 명백히 알수 있는바와 같이 이것은 공격자가 송신자와 수신자중 그 누구도 자기를 전혀 알아 차리지 못한채로 그들사이의 모든 통신을 읽고 수정할수 있도록 한다.

이 문제는 인증국(CA)을 리용함으로써 해결된다. CA는 송신자의 인증서와 수신자의 인증서에 수자식으로 서명한다. 인증서는 그 소유자들의 이름과 공개열쇠를 포함하는데 그것들의 무결성은 CA의 공개열쇠를 리용하여 검사할수 있다. 그러나 이것은 송신자와 수신자가 같은 CA에 속하여야 한다는것을 의미한다. 만일 송신자와 수신자가 같은 CA의 성원이 아니라면 CA들의 계층구조가 수립되여야 한다(그림 34－1 참고).

그림 34－1에서 매 실체는 계층구조의 보다 우에 있는 실체에 의하여 서명되는 자기자신의 인증서를 가진다. 이것은 알려 진 실체로부터 알려 지지 않은 실체에로 신뢰(trust)를 전달하는데 리용되는 방법이다. 례외로 되는것은 뿌리인데 이것은 자체로 서명되는 인증서를 만든다. 뿌리는 CA들과의 직접적인 교섭과 업무관계를 통하여 신뢰를 수립하여야 한다.

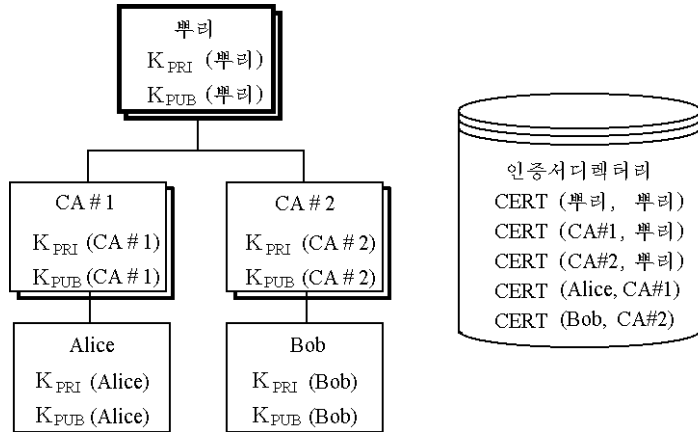



그림 34－1. 기초RKI계층구조

이 환경에서 Alice는 문서에 수자식으로 서명하고 그것을 자기 인증서의 복사본은 물론 CA#1의 인증서와 함께 Bob에게 보낼수 있다. Bob는 이미 CA#2와 믿음관계를 가지고 있고 CA#2는 뿌리와 신뢰관계를 가지고 있기때문에 Bob는 CA#2의 인증서를 확증하고 다음 Alice의 인증서를 확증할수 있다. 일단 Bob가 Alice의 인증서를 믿으면 그는 자기가 Alice의 공개열쇠로 확증할수 있는 임의의것이 Alice의 비밀열쇠에 의하여 서명되였을것이며 따라서 Alice로부터 왔을것이라고 믿는다.

뿌리열쇠타개의 후과

이 계층구조의 문제점은 뿌리비밀열쇠의 안전에 대한 전적인 믿음에 있다. 만일 K_{PRI}(뿌리)가 공격자에 의하여 타개되면 그 공격자는 기만적인 CA#3을 창조하고 그 다음 그 CA밑에 기만적인 사용자들을 만들어 놓을수 있다. CA#3이 뿌리의 공개열쇠를 리용하여 명확하게 확증될수 있으므로 Alice, Bob 그리고 뿌리를 믿고 있는 모든 사람들은 CA#3밑의 임의의 사용자들을 수락할것이다. 이로하여 Alice, Bob 그리고 이 계층구조에 있는 그밖의 모든 사람들은 기만적인 사용자들을 믿게 되며 바로 거기에 문제가 있다는 것을 알지 못하는 사태에 빠지게 된다.

만일 이런 일이 일어 난다면 전체 체계는 풍지박산이 된다. 믿음에 대한 기초가 허물어 졌으므로 그 어떤 거래도 진행할수 없게 된다. 이 사태로 하여 빚어 지는 보다 더 충격적인 후과는 Alice와 Bob가 그 문제에 대하여 알아 차리자마자 CA#3밑의 사용자들에 대한 믿음을 중단할뿐아니라 전체적인 계층구조에 있는 그 누구도 믿을수 없게 될것이라는것이다. CA#3이 기만적으로 창조되였으므로 기만적인 CA들은 몇개라도 만들어 질수 있으며 있을수 있는 CA들로부터 믿지 말아야 할 CA들을 결정하기 위한 아무러한 방도도 없다.

믿어야 할 CA들을 결정할수 없다면 믿어야 할 사용자들의 인증서를 결정하기 위한 방도가 더는 없다. 이것은 전체적인 계층구조를 우로부터 아래까지 완전히 붕괴시키게 된다.

암호기법적으로 안전한 수자식시간도장만들기

암호기법적으로 안전한 수자식시간도장(CSDT)은 결코 새로운것이 아니다. 여러해동안 안전한 시간도장을 넓은 분야에서 여러가지로 적용해 오고 있다. 이 장의 목적은 실제적인 CSDT를 만드는데까지 세부를 깊이 파고 들자는데 있는것이 아니라 오히려 수자식인증서안에 포함되는 최소한의 필요한 자료를 지적하자는데 있다.

시간도장

물론 CSDT의 기본구성요소의 하나가 시간도장 그자체이므로 《믿을수 있는》시간원천이 필요하다. 이것은 여러가지 인정된 방법으로 달성할수 있으며 이것을 만들기 위하여 CSDT내의 실제적인 시간도장은 정확한 시간이라는것을 가정할것이다.

대용량거래환경을 조성하기 위하여 동일한 시간에 두개의 CSDT가 있을수 없게끔 시간도장에 16bit순서번호가 붙여 진다. 이 타이브레이커값(tiebreaker value)은 새로운 매 시간도장마다 재설정되여야 한다. 따라서 시간분해능이 0.0001s라면 동일한 0.0001s내에 발행될수 있는 CSDT들의 가능한 개수는 모두 65,536개나 되지만 정확한 순서의 CSDT를 만드는것은 미래에 결정될수 있는 일이다.

인증서의 하쉬

특별한 인증서에 CSDT를 결합하기 위해서는 일부자료가 해당 인증서에 련결되도록 포함되여야 한다. SHA–1이나 MD5와 같이 이미 알려 져 있는 믿을만한 알고리듬에 의하여 생성되는 인증서의 하쉬는 이 련결을 보장하는데 리용된다. 이것은 인증국이 서명처리를 하는 동안 계산되고 암호화되는 바로 그 하쉬이다.

보다 중요하게는 CSDT의 시간은 CA가 인증서를 서명할 때의 시간이라는것을 아는것이 결정적인 문제이다. 따라서 그런 하쉬가 포함될것이 아니라 CA에 의하여 완전한 수자식서명이 인증서에 첨가되여야 한다. CA의 서명을 리용하여 또한 미래의 CA서명표준의 변화를 보장할수 있다.

그러나 이 장의 목적의 하나는 현존 인증서표준을 변경시킴이 없이 거기에 새로운 기능이 하나 더 추가되는것만큼 누구도 서명후 인증서에 정보를 추가할수 없다는것을 강조하자는것이다. 오히려 CSDT는 인증서가 CA에 의하여 서명되고 X.509v3확장마당에 삽입되기에 앞서 그 인증서에 추가되여야 한다.

인증국의 인증서하쉬

다른 하나의 추가적인 조치의 하나로서 CA의 인증서의 하쉬가 CSDT에 내장되여 어느 CA가 시간국(TA: Time Authority)에 요청하는가에 대한 기록을 제공한다.

시간국의 수자식서명

함부로 변경되는것을 막기 위하여 CSDT는 표준수자식서명을 리용하여 암호기법적으로 서명되여야 한다. CSDT의 전체 자료량이 작으므로 이것은 TA의 비밀열쇠로 자료마당들을 간단히 암호화하는것으로써 달성된다. 그러나 앞으로의 증대와 추가될수 있는 첨부마당들을 허용하기 위하여 안전하게 모든 자료의 하쉬들을 암호화하는것이 더 좋다.

계층구조의 분리

물론 X.509표준은 이미 시간도장을 포함하고 있으므로 자기 CA에 의하여 인증서가 서명된 날자와 시간이 결정될수 있다. 그러나 뿌리비밀열쇠가 타개되고 기만적인 CA가 만들어 지면 그 CA는 인증서를 서명하기에 앞서 시간을 요구되는 값으로 간단히 설정할 수 있다.

제안되는 한가지 방법은 CA를 자기의 부분으로 가지는 계층구조밖에 존재하는 어떤 국에 의하여 서명되는 시간도장을 포함하는것이다(그림 34－2 참고).

CA가 하나의 인증서를 만들 때 그것은 인증서에 포함될 공개열쇠와 다른 자료를 취득하기 위한 정상과정을 거친다. 그러나 인증서를 서명하기에 앞서 시간국(TA)으로부터 CSDT가 요구될것이다. 이 CSDT는 그때 TA에 의하여 생성되며 CA에로 귀환될것이다. CA는 CSDT를 인증서에 첨부하고 다음 보통의 방법으로 그에 서명할것이다.

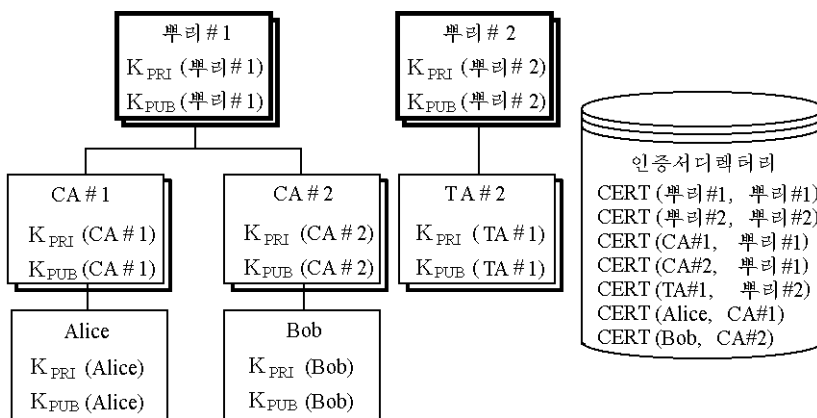



그림 34－2. 시간국을 가진 PKI

뿌리#1이 어떤 점에서 타개되면 뿌리 #1에로의 접근이 CSDT를 만들수 있는 능력을 주지 않으므로 타개되기전에 창조된 모든 CA들은 여전히 믿을수 있다. 그러면 사용자들은 특정한 날자후에 뿌리에 의하여 서명되는 그 어떤것도 믿을수 없지만 그 날자전에 서명된것은 아무것이나 믿을만한 가치가 있다는것을 알수 있게 된다.

CSDT를 포함하는 인증서발급절차

CSDT를 공개열쇠인증서에 첨부하는 절차는 다음과 같다.

1. 사용자가 공개/비밀 열쇠쌍을 생성한다.
2. 사용자가 공개열쇠와 사용자특정정보를 등록국(RA: Registration Authority)에 보낸다.
3. RA는 사용자의 요청을 정당하게 접수하고 CA에 인증서요청을 보낸다.
4. CA는 인증서를 형성하고 사용자인증서하쉬(UCH: User Certificate Hash)를 계산한다.
5. CA는 수자식으로 서명되는 요청을 UCH를 포함하고 있는 시간국에 보낸다.
6. TA는 요청을 접수하고 CA의 공개열쇠인증서를 리용하여 그 요청에 대한 CA의 서명을 정당화한다.
7. TA는 자기의 안전한 시간원천으로부터 현재 시간을 얻는다.
8. TA는 순서타이브레이커계수값을 계산한다.
9. TA는 CSDT의 내용을 다음과 같이 형성한다.
   ㄱ. UCH(절차 4)
   ㄴ. 시간도장(절차 7)
   ㄷ. 타이브레이커계수(절차 8)
   ㄹ. CA의 인증서의 하쉬(절차 6에 리용된것과 같은 값)
10. TA는 CSDT의 내용들의 하쉬를 계산한다.
11. TA는 자기의 암호열쇠로 하쉬를 암호화한다.
12. TA는 CA에로 CSDT를 귀환한다.
13. CA는 TA의 공개열쇠인증서를 리용하여 CSDT에 대한 TA의 서명을 정당화한다.
14. CA는 TA에 보낸 UCH와 대조하여 CSDT의 UCH를 검증한다.
15. CA는 사용자인증서에 CSDT를 첨부한다.
16. CA는 완성된 인증서에 관한 표준서명과정을 수행한다.
17. CA는 사용자에게 수자식인증서를 보낸다.

수 복 절 차

보증을 담보하는 임의의 체계에서는 일부 문제 있는 사건에 대처한 행동계획을 가지는것이 필요하다. CA가 타개될 때 최소한의 필요한 절차에 대한 요약을 아래에 준다.

주어 진것:

- CA뿌리에 의하여 서명된 CA
- TA뿌리에 의하여 서명된 TA

- 공개/비밀 열쇠쌍을 발생한 10,000명의 사용자
- 매 사용자는 공개열쇠인증서발급과정을 거쳤다.
- CA뿌리열쇠는 어떤 형태의 공격에 의하여 타개된다.

CSDT가 사용되지 않는 기반에서 10,000명의 사용자들의 인증서들은 모두 곧 문제시될수 있으며 그이상의 거래에 대하여 믿을수 없게 된다. 전형적인 계획은 CA가 미리 두번째 교체뿌리를 만들어 놓고 첫번째것이 배포되였으면 두번째 뿌리의 자체서명된 공개열쇠인증서가 배포될것을 요구한다. 그러면 사용자들은 첫번째 뿌리에 대한 신뢰를 중지해야 한다든지 또는 그것을 자기들의 응용프로그람에서 삭제해야 한다는것을 알게 된다. 그다음 모든 사용자들은 새로운 열쇠쌍을 생성하여야 하며 업무가 정상으로 돌아 오기전에 새로운 뿌리아래에 등록하는 과정을 거쳐야 한다.

이것은 명백히 상당한 시간과 로력을 요하며 전자업무거래를 실행하려는 사용자들에게 상당한 불편을 줄수 있다. 또한 사용자수가 증가함에 따라 수복시간은 선형으로 증가한다.

CSDT가 채용되고 CSDT인식응용프로그람들이 리용되면 그 많은 로력이 필요 없게 된다. 타개가 되였다고 판정되면 곧 다음과 같이 해야 한다.

- TA는 타개된 열쇠아래에서는 더이상 요청을 접수하지 않을것이라는것을 알아야 한다.
- 자기의 사용자들을 알아야 한다.
- 새로운 열쇠들의 조를 생성하여야 한다.
- 타개된 열쇠아래에서는 더이상 인증서들을 발급하지 말아야 한다.

사용자들은 CA에게 타개날자/시간이 있는 자기들의 응용프로그람에 대하여 무조건 알려 주어야 한다. 앞으로 모든 인증서의 타당성은 CA의 인증서는 물론 CSDT로 검사된다. 만일 인증서에 대한 CA의 서명이 타당하지만 CSDT가 없거나 타개된 후의 시간을 지적한다면 그 인증서는 거부되며 사용자는 자기들이 부당한 인증서를 가지고 있었다는것을 알게 된다.

알려 진 문제점들

하쉬생성, 암호화, 복호화와 같은 사건들은 령아닌 존속(non–zero duration)과정들이므로 실제적인 인증서발급시간은 CSDT내의 시간이 아니라는것이 인정되여야 한다. 이것은 CSDT내의 시간과 인증서자체내의 시간이 절대시간으로 리용되는것이 아니라 오히려 인증서가 타당하게 고찰되는 시작점으로 리용되므로 문제시될것은 없다.

임의의 암호화체계와 같이 체계의 임의의 타개에 대한 시기적절한 지식은 공격자의 어떤 《행운의 기회》를 제한하는데서 중요한 요인으로 된다. 이런 경우 CA야 말로 자

기 사용자들에게 자기가 타개당하였다는것을 알려 주어야 한다. TA의 타개에 관한 정보도 역시 사용자들에게 알려 져야 하지만 그 결과로 어떤 직접적인 행동을 할 필요는 없다.

CA의 근본책임의 하나는 그 CA서명을 믿으려는 모든 사람들이 그 CA의 공개열쇠 인증서에 접근하도록 하는것이다. 이것은 역시 TA에서도 마찬가지인데 TA는 자기의 공개열쇠들에서 믿음을 수립하기 위한 류사한 방법들을 리용하여야 한다. 이것은 CA와 그 사용자들에게 추가적인 부담을 줄수 있다.

요 약

이 장에서 제안되고 론의된것은 지금까지 존재하지 않았던 PKI에서의 여유를 제공하는 방법이다. 뿌리비밀열쇠를 여러 부분으로 분할하는 이전의 방법들은 단일점고장에 대한 2중조종을 만들어 내였지만 어떤 체계적인 여유를 제공하지는 못하였다.

이 체계는 PricewaterhouseCoopers에 의하여 수립된 신뢰성 있는 제3자봉사업체인 beTRUSTed로부터 원형이 만들어 지고 있다는것에 주목할만한 가치가 있다. 여러 PKI쏘프트웨어업체들과 협동하여 검사해 보면 실지환경에서 이 체계의 리용성과 안전성을 증명할수 있다.

임의의 암호화체계나 규약의 사용과 같이 여기에 서술된 CSDT들을 사용하고 있는 체계는 가능한 취약점들이나 공격자가 체계를 타개할수 있는 부분들을 찾아 내기 위하여 제3자들에 의하여 분석되고 검사되여야 한다.

참 고 문 헌

1. Improving the Efficiency and Reliability of Digital Timestamping, http://www.surety.com/papers/BHSpaper.pdf.
2. How do Digital Timestamps Support Digital Signatures?, http://x5.net/faqs/crypto/q108.html.
3. Digital Timestamping Overview, http://www.rsa.com/rsalabs/faq/html/7-11.html.
4. How to Digitally Timestamp a Document, http://www.surety.com/papers/1sttime-stampingpaper.pdf.
5. Answers to Frequently Asked Questions about Today's Cryptography, v3.0, Copyright 1996, RSA Data Security, Inc.

제6편
보안구성방식과 모형

이 편에서는 자료기지의 무결성에 관한 중요한 문제를 취급한다. 저자는 자료기지무결성의 정의와 개념들을 론의한 다음 자료기지관리프로그람을 실행하며 자료기지의 무결성을 보존하는 방법을 설명하였다. 이 편의 결론으로부터 자료기지무결성은 임의의 보안계획의 본질적인 요소라는것을 상기할수 있다. 끝으로 자료기지의 무결성을 보존하는것과 관련한 저자의 권고는 정확성과 어느정도 류사한 체계의 무결성을 믿을수 있게 하는 어려운 목표에로 안내하는 《료리책》의 역할을 할것이다.

제35장. 자료기지의 무결성에 관한 고찰

윌리엄 휴 머리

이 장에서는 자료기지의 무결성과 관련된 개념을 고찰한다. 이 장에서는 자료기지무결성의 개념을 자료무결성 및 자료기지관리체계무결성의 개념과 대비적으로 설명한다. 그 목적은 자료기지의 소유자들과 운영자들에게 무결성을 보존하는 방법과 관련한 일련의 권고를 주자는데 있다.

개념 및 해설

여기서는 자료기지무결성과 관련된 문제들을 해설하며 또 그 문제에만 국한된 일부 정의들과 개념들을 서술한다.

무결성

무결성은 전일적이고 완결되여 있으며 손상이 없다는 의미의 속성이다. 다시 말하면 외부적인 간섭이나 오염이 없고 깨뜨릴수 없으며 요구조건이나 기대를 만족시킨다는 의미를 내포한다.

자료는 그것이 내부적으로 일관성을 가질 때(가령 책들이 잘 편성되여 있을 때)와 그 목적하는바를 반영하고 있을 때(가령 책들이 기업활동과 조건을 정확하게 반영하고 있을 때) 무결성을 가진다고 말할수 있다. 체계인 경우에는 그것이 대부분의 시간을 완결된 기술설명서에 따라 동작하고 예측할수 있는 오동작을 하며 그 오동작의 원인이 명백하여 그것을 제때에 효과적으로 퇴치할수 있으며 그리고 순차적으로 회복할수 있을 때

무결성을 가진다고 말할수 있다.

자료기지

무결성의 견지에서 보면 자료기지는 련관된 혹은 호상 의존하는 자료요소들의 전일적인 집합으로 정의할수 있다. 달리 표현하면 자료기지는 코드화된 자료요소들과 그 요소들사이의 구체적인 관계로 표현되는 정보의 전일적인 집합이다. 자료기지는 사용자, 사용 혹은 응용프로그람사이에서 공유된다.

자료기지의 추상화는 비교적 새로운것이며 현대콤퓨터와 거의 시기를 같이 한다. 약 10년전 마이크로콤퓨터용의 자료기지관리쏘프트웨어가 출현할 때까지 자료기지의 추상화는 해석하기 어려웠다. 콤퓨터가 출현하기전에도 기업활동과 관련한 영업회계장부와 같은 상사형자료의 집합들이 존재하였다. 자료기지라는 용어는 대장카드나 3×5카드와 같은 매체에 일반적으로 기록되는 대부분자료들에 적절하게 적용할수 있다. 그렇지만 최대한의 형식성과 엄밀성 그리고 체계성을 가진 자료집합들에 한해서만 흔히 자료기지라는 말을 쓴다.

자료기지에서 정보는 코드화된 자료요소형식으로 명시적으로 표현될수 있다. 종업원이름이 일반적인 실례로 된다. 그러나 자료기지에는 자료요소들사이의 명시적인 혹은 암시적인 결합형식으로 표현되는 다른 정보도 있다.

관계는 자료요소들사이의 특수한 결합방식이다. 례를 들어 종업원자료기지레코드의 각이한 마당(field)은 종이우에서와 꼭같이 론리적으로 련관된다. 매개 마당의 의미와 개체성(identity)은 부분적으로는 그 문맥에 의하여 결정된다. 이 정보는 최소한도로 자료요소자체에서의 정보만큼 중요하다.

관계는 자료 그자체(관계자료)에서 표현되거나 자료기지(구조화된)안에서 요소들의 배렬이나 순서로 표현되기도 하며 관계(가령 색인순차관계 혹은 객체지향관계)를 명시적으로 표현하거나 부호화하는 자료에 대한 자료라고 할수 있는 메타자료에서도 표현될수 있다. 자료기지는 관계들이 원래 어떻게 표현되는가(표현방법)에 의하여 특징지어 질수 있지만 실천적으로 모든 자료기지들은 결합된 관계를 리용한다. 례를 들어 관계형자료기지라고 하는 자료기지에서 일부 관계는 구조(즉 표나 그림)로, 일부는 자료(즉 다른 표에 대한 참조)로 그리고 일부는 메타자료 즉 렬들의 이름으로 표현된다.

자료기지무결성

자료기지는 그것이 정보를 자료로 보존할 때 즉 자료와의 관계가 유지될 때 무결성을 가진다고 말할수 있다. 자료기지무결성은 레코드(기록)들의 무결성을 의미한다. 자료기지무결성은 한편으로는 자료의 무결성, 다른 한편으로는 자료기지관리체계의 무결성과 독립적이며 따라서 대조될수 있다.

자료기지관리체계

자료기지무결성의 견지에서 자료기지관리체계는 자료기지를 구축하고 유지하며 기억

하고 보존하며 응용프로그람에 자료기지를 제공하고 또한 응용프로그람을 대신하여 자료기지를 제공하는 일반적이고 추상적이며 자동화된 체계를 의미한다.

자료기지관리자는 자료요소들사이의 관계를 표현하기 위하여 그것들이 주로 의거하는 방식의 이름으로 특징지어 진다. 즉 두 자료요소사이의 관계가 표준적으로 자료자체 례컨대 자료요소의 내용(두 종업원레코드는 같은 부서번호를 가진다)이나 혹은 자료의 순서(종업원 A는 이름마당의 분류순서에서 B보다 앞에 놓인다)를 담은 자료기지관리자를 **관계형자료기지관리자**라고 부른다. 관계가 두개의 요소들이 물리적으로 보관되는 방식(례를 들어 같은 부서안의 모든 종업원들의 이름은 함께 기억되거나 혹은 종업원 A는 항상 B앞에 배렬된다)을 담은 자료기지관리자를 **구조화형자료기지관리자**라고 부른다.

관계무결성

관계무결성(Relational Integrity)은 자료요소들사이의 특수한 관계를 보존하는 자료기지무결성의 한 측면이다.

참조무결성은 관계무결성의 한 실례이며 특수경우이다. 참조(reference)는 한 레코드의 값이 일반적으로는 레코드형이 다른 레코드를 지적하는 관계이다. 자료기지무결성의 견지에서 참조는 자료기지가 관계를 보존할 정도로 무결성을 가진다고 말할수도 있는 하나의 실례이며 동시에 례증으로 된다.

레코드안에 부서번호가 있는 종업원레코드(부서레코드라고 부르는)의 경우를 고찰하자. 만일 종업원레코드에서 부서번호가 N이라면 그때 참조무결성은 부서 N에 대한 부서레코드가 있을것을 요구한다. 참조무결성은 대응하는 부서레코드가 없었던 부서번호를 가지는 종업원레코드의 구축, 임의의 종업원레코드가 부서레코드 N을 지적하는 한 그것(부서레코드 N)의 삭제 그리고 종업원레코드가 지적하는 하나이상의 부서레코드 N을 금지할것이다.

지적하여야 할것은 이 류형의 무결성은 요구에 따라서만 가능하다는것이다. 즉 그 어떤 공식적인 요구나 필요성, 법적실행이 없이도 그런 참조무결성의 조건들이 우연히 지어 지는 경우도 있다는것이다. 또한 무결성은 응용프로그람이나 자료기지관리체계를 리용하여 실현되거나 시행될수 있다. 일반적으로는 자료기지가 응용프로그람들에서 공유될수 있도록 그리고 응용프로그람을 리용하는 자료기지가 다른 자료기지에 의존할 필요가 없도록 자료기지관리체계에서 참조무결성을 실현하는것이 더 좋다.

방　법

이 부분에서는 자료기지관리자를 실현하며 자료기지의 무결성을 보존하는 몇가지 방법들을 론의한다.

국부화

정의에 따르면 자료기지는 전일적인 집합체이다. 다시 말하면 자료기지의 모든 요소

들과 모든 관계들은 그 자료기지의 개체성에 관하여 필수적이다. 만일 임의의 요소나 관계가 분실되거나 파손된다면 그때 개체성과 무결성은 파괴된다. 물론 이것은 둘 혹은 그 이상의 독립적인 자료기지를 포함할수 있는 물리적인 자료기지관리자와 독립이다. 그렇지만 모든것들은 같으므로 자료기지의 요소들을 다 함께 보관하면 자료기지의 무결성을 보존하는데 도움이 된다. 그러므로 대부분의 자료기지관리자들은 자료기지를 다 같은 곳에 국부적으로 보관하려고 한다.

단일소유과정

국부화의 중요한 형식의 하나는 단일소유과정이다. 자료기지는 전일적인 집합체이므로 자료기지안의 모든것들을 관찰하고 자료기지를 관리하여 자료기지의 무결성을 책임지는 단일한 과정이 분명히 있어야 한다. 이 단일과정을 관리하는 프로그람이 자료기지관리자이다.

여유자료

자료기지를 보관하는 매체와 장치들보다 자료기지를 더 믿음성 있도록 하기 위하여 대부분의 자료기지관리자들은 어떤 류형의 여유자료를 사용한다. 그 자료는 그것을 다른 방법으로 표현하는데 필요한 최소비트수보다 더 많은 비트수로 기록된다.

동적인 오유검출과 수정

보통 여유자료는 오유검출코드와 수정코드의 형식을 가진다. 그 자료는 한 비트의 변경을 명백히 알게 하며 그 변경을 제때에 그리고 자동적으로 수정할수 있게 하는 코드에 기록된다. 기우성(parity)이 바로 이런 코드의 하나인데 그 코드에서는 7bit 혹은 8bit로 구성된 매개 프레임에 보충적인 비트가 추가되여 그 프레임이 짝수 혹은 홀수와 같은 어떤 임의의 규칙에 일치되게 한다. 그 규칙으로부터의 편기는 한 비트가 변경되였다는 신호를 발생한다. 일부 코드들은 다중비트오유들을 자동적으로 검출하고 수정할 정도로 효과적이다. 이 코드들은 기억장치나 혹은 자료기지관리자에 의하여 실현될수 있다.

복사

여유자료는 자료기지나 자료기지요소들이 여러번 완전히 복사(copy)되는 회수만큼 옮겨 질수 있다. 이러한 복사는 자료기지관리자(프로그람)안에서나 밖에서 진행될수 있다. 관계는 일반적으로 자료기지관리자에게 가장 잘 알려 지므로 자료기지관리자가 제공하는 복개별비를 리용하면 가장 잘 보존된다.

거울화

거울화(mirroring)는 복사의 한 형태로서 거기서는 두개의 동기화된 복사자료가 유지

된다. 거울화는 자료기지안에서 진행되며 따라서 자료기지밖에서는 그 복사자료를 볼수 없다. 례를 들어 파일관리자가 파일을 거울화할수 있다. 파일관리자는 변경내용을 두 복사본에 다 적용하고 두 복사본으로부터의 요청을 만족시키지만 자료기지밖의 공정에는 두번째 복사자료가 존재하는것을 숨긴다. 거울화는 한 장치나 서로 다른 장치에서 진행될수 있다. 한 장치에서 진행될 때 거울화는 매체고장이나 장치의 제한된 고장(가령 불량자리길)이 있어도 자료를 보호한다. 장치들사이에서 진행될 때에는 일반적인 장치고장이 있어도 자료를 보호한다.

예비복사

자료기지의 예비복사(backup)는 자료기지관리자에 무관계하게 진행된다. 다른 손실들 가운데서 이 복사본은 특수하게 관리자가 실수하거나 부주의로 하여 있을수 있는 손상으로부터 자료를 보호한다.

이러한 복사는 자료기지관리자나 자료기지자체에 무관계한 편의프로그람 혹은 다른 프로그람공정들에 의하여 자동적으로 준비될수 있다. 물론 비록 자료기지고장이 있어도 보호하기는 하지만 독립적인 예비체계를 리용하는것은 그 자체가 자료기지의 무결성에 대한 위협으로 될수 있다. 독립적인 체계는 자료기지관리자자체가 집행하는 규칙을 알고 집행하기는 어렵다.

검사점과 실행기록

검사점은 예비복사의 특수경우이다. 검사점은 특수한 점에 제때에 설정된다. 례를 들면 자료기지의 초기상태는 가령 비여 있다 해도 검사점이다. 검사점들은 그에 뒤따르는 모든 갱신활동의 실행기록(journal)이나 운용기록(log)과 관련하여 리용되여 자료기지를 재구성한다. 이 방식에서는 무결성과 현행성(currency)이 둘 다 보존된다.

재구성

큰 고장이 있는 경우에는 이러한 2차적인 복사본들을 리용하여 자료기지를 재구성할수 있다. 그러나 이것은 일부 경우에는 자료기지의 무결성이 이런 2차복사본의 무결성에 더 의존할것이라는것을 의미한다.

구획화

구획화한다는것은 사물들을 분리된 구획들에 배치한다는것이다. 그 목적은 한 구획에서 생기는 결과들을 포함함으로써 이 결과에 의하여 다른 구획들이 영향 받지 않게 하는것이다. 례를 들어 단일한 큰 자료기지관리자에 앞서 여러가지 작은 자료기지관리자들을 실행하여 고장의 영향을 제한하도록 할수도 있다.

분리와 독립성

자료기지관리체계들은 무결성을 보존하기 위하여 흔히 부분공정들의 분리 및 독립성을 실행한다. 례를 들면 자료기지관리체계들은 갱신을 실행하는 공정, 갱신이 정확히 진행되였는가를 검사하는 공정, 수정작용을 하는 공정들을 모두 분리한다. 그 목적은 한 고장이 세개의 공정에 다 영향을 줄 가능성을 최소화하자는데 있다.

교갑화

자료기지관리자는 자료기지를 외부적인 간섭이나 오염으로부터 보호하는 역할을 하는 묶음, 용기 혹은 교갑으로 볼수 있다. 교갑화(encapsulation)는 물리적인것이거나 혹은 론리적인것일수 있다. 자료기지관리자인 경우 물리적인 교갑화는 자료기지관리자를 개별적인 콤퓨터에 배치하는 방법으로 보장될수 있다. 론리적인 교갑화는 자료기지관리자를 공유된 콤퓨터와 그 조작체계가 제공하는 환경내에서 분리되고 보호된 공정에 배치하는 방법으로 보장될수 있다. 론리적인 교갑화는 또한 부분적으로 정적인 조건에서 비밀코드(secret code)에 의하여 보장될수 있다.

대부분의 자료기지관리체계들은 자료기지의 일정한 교갑화를 제공한다. 객체지향자료기지관리체계들은 정의에 의하여 명시적으로 그리고 전반적으로 그런 교갑화를 제공한다. 앞으로 자료기지관리자자체가 그 하드웨어에서 교갑화되고 있다는것을 보게 된다.

숨기기

교갑은 자료기지의 내용들을 외부에서 보거나 리용하지 못하도록 숨긴다. 이것은 자료기지를 파괴면에서는 더 안전하게 하지는 못하지만 비법적인 로출과 의도적이면서도 눈에 띄지 않은 변화로부터 그 내용들을 보호한다. 숨기기(hiding)는 여러가지 방법으로 실현될수 있다. 가장 일반적인 방법은 공정의 호상분리, 자료형만들기 및 자료형관리자에 의한 방법과 비밀코드를 리용하는 방법이다.

맺기

맺기(binding)는 가령 자료특성이나 혹은 참조가 후에 변화되지 않도록 결정하고 고정하는데 리용된다. 콤퓨터과학에서는 초기맺기와 마감맺기라는 말을 사용한다. 례를 들면 일부 프로그람작성에서는 기호적이름들이 콤파일될 때 변화되지 않도록 맺어 지며 한편 다른 프로그람작성에서는 같은 특성들이 실행될 때까지 맺어지지 않을수 있다.

많은 구조형자료기지관리체계들은 프로그람작성이나 프로그람적재시에 관계들을 자료기지에 맺는다. 이렇게 하면 유연성은 손실되고 유지비용은 증가되지만 무결성과 성능을 개선할수 있다. 관계형자료기지관리자들도 역시 자료기지구축에 표형태의 맺기를 채용한다.

맺기는 그것이 진행되는 환경내에서만 적용된다. 만일 자료나 자료기지가 자료기지관리자로부터 분리되면 그때 특성들은 더는 맺어 지지 않으며 믿을수 없다.

미세갱신

미세갱신(atomic update)이란 자료기지의 임의의 변화가 전일적으로 발생하거나 전혀 발생하지 않는다는것을 의미한다. 부분갱신이란 없다. 미세갱신은 자료요소와의 관계를 포함한다. 대부분의 자료기지관리자들은 전일적으로 완결될수 없는 임의의 부분적인 갱신을 이른바 《복구》하는 능력을 유지하는 방법으로 미세갱신을 실현한다.

잠그기

자료기지무결성에 대한 잠재적인 위협의 하나는 둘 혹은 그이상의 공정에 의한 동시적인 리용으로부터 생긴다. 례를 들면 두 사용자가 자료기지를 변화시킬 때 두번째 변화가 첫번째 변화에 덧씌워 질 가능성이 있다. 자료기지관리체계는 이러한 문제의 발생을 막는 잠그기(locking)와 같은 기능들을 제공한다.

잠그기는 부분적으로 갱신될 요소들과 관계들이 리용되지 않는다는것을 담보하기 위하여 자료기지관리자들이 채용하는 하나의 기능이다. 이 기능에 의하여 요소에 《사용중》이라는 표식이 붙거나 갱신되는 모든 요소들에 《잠그기요구》라는 표식이 붙는다. 이 기능은 사용중에 있는 요소의 두번째 리용을 허용하지 않으며 갱신되는 모든 요소들이 잠그어 질 때까지는 갱신을 시작하지 않는다. 그렇지만 잠그기는 보통 물리적인 기능이라기보다는 오히려 론리적인 기능이다. 잠그기는 일반적으로 잠그기 혹은 열기로 설정되는 한비트 혹은 기발이다.

잠그기는 투명성과 세립성의 여러 준위로 진행할수 있다. 리상적으로는 잠그기는 자동적이고 모든 사용자들에게 있어서나 공정의 리용에 있어서 투명하다. 그러나 이 방법은 필요없이 성능에 영향을 줄수도 있다. 례를 들면 투명성이 최대인 경우 자료기지관리체계는 응용프로그람 A가 갱신을 위하여 선택된다는 가정하에서 응용프로그람 A가 관리하는 임의의 자료에로의 접근을 응용프로그람 B가 못하게 제한할수 있다. 결국 응용프로그람 B는 잠재적인 갱신을 고려하지 않는다 해도 성능은 떨어 질것이다.

성능은 또한 응용프로그람 B의 접근이 응용프로그람 A가 갱신할수 있는 최소의 요소에만 국한될것을 요구한다. 응용프로그람 B는 다만 응용프로그람 A가 표의 단 하나의 행에 관심하기때문에 전체 표로부터 제한을 받아서는 안된다. 결국 최대성능은 A와 B가 자기의 목적을 선포할것을 요구한다.

접근조종

접근조종은 자료기지의 관리자들로 하여금 사용자나 사용하는 공정들이 자료기지와 그 요소들 혹은 그 관계를 변경시키는것을 조종할수 있도록 자료기지관리체계에 의하여 제공되는 기능이다. 이 조종은 다중사용자들이 리용할수 있도록 자료기지관리체계에 포함시키는것이 가장 좋은것 같다. 그 조종은 자료기지를 변경시킬수 있는 사용자의 수를 계획된 수로 변화시킨다는 점에서 하나의 무결성기능이다. 그것은 또한 오유나 악의(malice)를 막기 위한 이중통제를 실행하는데 리용된다.

특권적조종

대부분의 자료기지관리체계들 특히 접근조종을 제공하는 자료기지관리체계들은 특권적조종기능을 제공한다. 이 특권적조종의 목적은 체계관리자들이 리용하기 위한것이다. 이 조종은 궁극적인 조종을 실행하기 위하여 특히 비정상적인 상태를 수습하기 위하여 리용된다. 두가지 비정상적인 상태가 특별히 주목된다. 첫번째는 접근조종을 무효로 하는 것이다. 이 능력은 교착(deadlock)상태를 피하기 위하여 필요할수 있다. 두번째는 자료기지 그 자체를 보수하기 위한 특권의 리용이다. 초기의 구조화된 자료기지에서는 《파손된 사슬을 보수》하기 위하여 이러한 조종들을 리용하였다.

지적하여야 할것은 이런 특권적조종이 자료기지를 오염시키거나 자료기지에 간섭할수 있다는것이다.

조정

조정(reconciliation)는 자료기지를 조화 혹은 일치되게 하는 작용이나 공정을 가리킨다. 즉 자료기지를 검사하고 그 변화를 수정하는 작용 혹은 공정을 가리킨다. 일반적으로 자료기지관리체계들은 이러한 검사를 루틴(부분프로그람)에서 자동적으로 자주 그리고 완전히 련속은 아니지만 반복적으로 실행한다. 례를 들면 다른 공정(례컨대 파일체계)에 쓰기요청을 한후 자료기지관리자는 그 요청이 정확하게 완결되였는가를 확인하기 위하여 즉시 검사를 할수 있다. 루틴과 이 활동의 자동적인 특징으로 하여 조정은 회복과 구별된다. 다른 차이점은 조정이 거의 전용적으로 내부자원에 의거한다는것이다.

회복

회복(retrieval)은 무결성기능의 마지막수단으로서 자료기지가 그것을 보수할수 있는 어떤 다른 기능의 능력이상으로 파손되였을 때 리용된다. 회복은 일반적으로 외부적으로 요청되며 자료의 예비복사와 같은 외부자원에 의거한다. 회복은 자료기지를 무결성상태로 회복시키는 반면에 돈이 많이 들고 지어 자료를 잃게 할수도 있다.

결 론

자료기지무결성은 본질적인 속성이다. 만일 자료에 의거할수 없다면 자료기지는 리용할수 없다. 무결성은 보존하기는 쉬워도 다시 창조하기는 힘들다. 하나의 도구나 기능만 가지고는 안된다. 자료기지관리체계는 다양한 도구들을 리용하며 소유자와 관리자들은 완전히 외부적인 도구들을 채용하여 자료기지관리자의 고유한 제한성을 메꾸어 주어야 한다.

자료기지의 무결성을 보존하자면 적어도 다음과 같은 네가지 사항이 필요하다.

1. 자료요소들과 그리고 그것들사이의 관계를 다 보존해야 한다.
2. 자료기지관리체계가 제공하는 기능들을 리해하고 리용하여야 한다.
3. 이 기능들중 임의의 기능을 그 리용과정에 또는 외부적으로 손상시키지 말아야 한다.
4. 자료기지관리체계의 제한성을 리해하고 그것을 보상하여야 한다.

자료의 단순한 복사로는 관계에 포함된 정보를 보존하지 못할수도 있다. 례를 들면 만일 구조화된 자료기지가 장치안에서 자료의 물리적위치관계에 대한 정보를 포함한다면 그때 자료의 복사는 자료가 같은 장치에 있을 때에만 그 관계를 보존할수 있다.

모든 자료기지관리체계들은 기능들의 결합으로 관계를 실현하며 그 기능들의 대부분이 숨겨 지므로 자료기지관리체계를 우회하는 운영절차나 관리는 의심스럽다. 한편 자료기지관리체계와 무관계한 무결성을 보존하는 다른 대책이 없다면 한 기능의 고장으로 자료기지가 파괴될수 있다.

주의하여야 할것은 대부분의 견고한 자료관리자들은 자료기지를 교갑화하므로 그 관리자들을 우회할수 없다는것이다. 자료기지관리자를 우회하려는 임의의 시도는 극상해서 자료기지를 외곡하지만 최악의 경우에는 자료기지와 자료기지관리체계를 파괴시킨다. 대부분의 자료기지관리체계들은 또한 자료기지의 외부적표현을 구축하는 여러개의 내장기능들을 제공한다.

마지막으로 언급할 문제는 규모(scale)문제이다. 대부분의 자료기지들은 그것들을 상주시키는 체계나 장치에 비하면 상대적으로 작다. 그러나 가장 중요한 자료기지들가운데서 많은 자료기지들은 대단히 크며 수십 혹은 지어 수백개의 장치들을 망라한다. 이러한 자료기지에서 관계에 관한 정보는 많은 장치들을 망라할수 있다. 자료기지의 무결성은 장치들과 장치들사이의 관계를 보존할것을 요구한다.

한편 이 자료기지들에서는 자료기지나 파일이 아니라 오히려 예비장치복사에 의하여 외부적인 복사본들을 구축하는것이 일반적이다. 이러한 예비복사는 장치 및 장치마당에 종속된다. 이 예비장치들은 하나 혹은 두개의 장치들이 고장나도 적당한 보호를 제공하는 반면에 전체 환경이 파괴되는 경우 회복하자면 그 환경의 완전한 재현을 요구할수도 있다. 이 재현은 며칠 혹은 지어 몇시간안에 진행되여야 한다. 그러므로 장치와 독립적인 예비복사를 해두는것이 가장 절실한 자료기지들에서는 외부적인 장치예비복사가 적당치 않을수 있다.

권 고 사 항

이 부분에서는 자료기지의 무결성을 보호하는것과 관련한 몇가지 권고를 제시한다. 이 권고에는 자료기지관리체계의 리용과 그 제한성을 극복하는것과 관련한 일부 권고들이 포함된다.

1. 특징, 기능, 속성들이 목적한 응용프로그람이나 환경에 충분히 견고한 자료기지관리자를 선택하시오.
2. 지도서에 따라 자료기지관리체계를 리용하시오. 모든 제한성을 지적하고 고려하시오.
3. 자료기지와 자료기지관리자를 견고한 환경에 배치하시오.
4. 응용프로그람이나 환경에 의하여 지적된대로 충분한 자원들(례컨대 거울파일, 장치 그리고 조종부들)을 제공하시오.
5. 무결성을 위해서는 전일적인 자료기지를 선택하시오. 성능에서의 기본차이에 의하여 허용된 정도로만 분산형자료기지관리자를 리용하시오.
6. 무결성을 위해서는 자료기지와 자료기지관리체계 그리고 처리기사이의 일대 일관계를 선택하시오. 규모의 경제성(economy of scale)에 의하여 지적된 정도만큼 공유하시오. 명심할것은 오늘날의 콤퓨터체계들은 그 응용에 따라 더 쉽게 규모가 조절될수 있다. 대규모의 공유로는 더는 종래의 경제성을 유지할수 없다.
7. 무결성을 위해서는 관계형 및 객체지향형자료기지를 선택하시오. 성능측면에서는 구조화된 자료기지쪽이 더 좋다.
8. 응용프로그람이나 사용자들은 그것이 의거하는 자료기지관리자의 동작을 검사하여야 한다.
9. 자료기지와 자료기지내부요소에로의 접근을 응용프로그람과 관계되는 최소수의 알려 진 사용자와 공정으로 제한하시오.
10. 접근조종은 자료기지에 대한 기밀정보를 갱신하는데 여러 사람들이 참가하도록 적용하시오.
11. 우선권조종을 리용할 때에는 많은 사람들을 포함시키시오.
12. 검사점과 갱신활동의 실행기록을 포함하여 여러개의 자료예비복사본과 자료갱신본을 보관하시오.
13. 특히 여러개의 장치들을 망라하는 자료기지에 대하여서는 장치와는 독립적인 예비복사쪽을 선택하시오.
14. 장치의 독립성과 관련하여 자료기지관리자가 제공하는 봉사에 의한 예비복사를 하는것이 좋다. 성능측면에서는 독립적인 기구들을 리용하시오.
15. 관계의 보존과 관련하여 자료기지관리자가 제공하는 봉사에 의한 예비복사를 하는것이 좋다. 독립성을 위하여 그리고 기구의 고장이 있어도 복사하기 위해서는 다른 수단에 의하여 예비복사를 하는것이 더 좋다.
16. 자료기지를 외부에서 복사하는것을 막기 위해서는 그 관리에 여러 사람들을 인입하시오.
17. 회복후와 리용하기전에 무결성을 검사하시오. 부식된 자료기지를 표준적으로 리용한다고 해도 그 손상이 퍼지며 불량자료를 리용하면 기업에 심중한 손해가 초래된다는것을 명심하시오.

제7편
운 영 보 안

운영보안은 보통 자료쎈터를 위주로 볼수 있지만 그 개념은 지난날의 개념이다. 현재 그 개념은 례컨대 모든 형태의 자료처리조작에 대한 행정적관리와 분산운영은 물론 집중운영의 보안개념, 운영조종의 각이한 선택, 자원보호요구사항, 회계운영, 감시 및 침입탐지를 비롯하여 훨씬 더 많은 내용들을 포함한다. 이 편에서는 침입해석과 그리고 일반적인 자료중심문제와는 거리가 먼 전자상업거래환경에서의 회계에 중심을 둔다.

지능적인 침입해석을 고찰한 36장에서는 사유하는 기계가 콤퓨터침입을 어떻게 인식하는가 하는데 대하여 론의한다. 현재의 판매품인 침입탐지체계를 리용하는 경우에도 련방법무성통계자료에 의하면 체계행정관리자가 탐지하는 매개 침입에 대하여 침입탐지체계는 10번 탐지한다. 완전한 예방대책은 기대할수 없으므로 탐지방법(가령 침입탐지체계)들이 준비되여야 한다. 이 장의 목적은 다음과 같은 세가지이다. 즉 문제해결에 인공지능의 리용을 촉구하는것, 인공지능의 기초개념들을 소개하는것 그리고 침입해석에 대한 인공지능의 리용을 탐구하는것이다. 이 장에서는 인공지능을 리용하여야 할 리유를 고찰한 다음 인공지능의 기초개념들을 소개한다. 지식의 역할, 침입탐지수법들, 신경회로망과 신경회로망의 학습능력 그리고 각이한 공격탐지에서의 그 리용에 대하여 고찰한다.

37장에서는 전자상업거래환경에서의 안정성 및 신뢰성의 중요성에 대하여 해설한다. 거기에서는 전자상업거래, 상업적거래방법과 관련된 위험을 정의한다. 또한 효률적인 전자상업거래개발에서 전략이 기본열쇠라는것을 서술한 다음 그 의미를 론의한다. 법적인 내적관계는 하나의 난점으로 언급된다. 전자상업거래구조의 구성성분들에 대하여서도 상세하게 서술한다. 전자상업거래환경에서 일하는 사람들이 전자상업거래운영을 성과적으로 보호하자면 배워야 할것이 많다.

제36장. 지능침입분석

브라이언 피쉬

위험관리는 정보보안의 기본이다. 가장 바람직한 수법은 위험을 총체적으로 피하든가 혹은 련관된 위협들이 발생하는것을 막는것이다. 예방대책도 중요하지만 때때로 예방대책도 보안사고를 막지 못한다. 이것을 고려하자면 기관들이 자기들의 보안방책들이 위반되는것을 식별하고 대응할수 있어야 한다. 완전한 위험완화전략은 예방대책들을 보충하는 탐지 및 수정대책들을 포함하여야 한다. 이 장에서는 침입을 탐지하는 인공지능기술에 대하여 조사한다.

침입이 무엇으로 구성되는가에 대한 지식은 합법적인 활동과 침입을 구별하는 기본열쇠이다. 그 지식을 기계가 리해하는 방식으로 표현하기는 어려우며 결국 침입탐지문제는 콤퓨터로 해결하기 어려운 문제이다. 대조적으로 대부분의 보안전문가들은 이러한 지식들을 소유하고 있으며 따라서 쉽게 침입을 탐지할수 있다. 오늘날의 정보체계능력은 규모가 큰 분석진영도 압도하기때문에 침입을 수동적으로 분석한다면 원가가 맞지 않는다. 필요한것은 수동적인 침입분석의 지식과 정확성을 콤퓨터의 능력 및 효률성에 결합시키는 체계이다.

이 장에서는 침입탐지체계로서 전망이 있는 일부 인공지능(AI)기술들을 고찰한다. AI의 기본개념들을 소개한 다음 AI기술이 침입탐지문제에 적용되는 한가지 방식에 대하여 깊이 조사한다. 그 목적은 다음과 같다.

1. AI를 리용하여 문제해결수법을 전반적으로 고찰하는것,
2. AI의 기본개념들을 소개하는것,
3. AI에 의한 침입분석을 탐구하는것.

첫번째 목적은 전통적인 기계처리과정을 인간의 사고와 대비하는 방법으로 론의한다. 그리고 두번째와 세번째 목적은 침입탐지의 효률성과 정확성을 개선하는 AI에 기초한 방법들에 대한 현재의 연구결과들을 론의하는 방법으로 고찰한다.

인 공 지 능

인간의 지능은 행성우에서 가장 위력하고 견고한 체계의 하나이다. 수년간의 연구를 통하여 과학자들은 지능에 대하여 많은것을 알게 되였으며 콤퓨터와 인간의 지능사이의 두드러지는 차이를 발견하게 되였다. 인공지능(AI)연구에서는 현재 인간에 의하여 최량적으로 수행되는 과제들을 콤퓨터가 더 능란하게 풀수 있는 방법을 개발한다.

지능의 리해와 관련하여 세가지 형태의 과제 즉 일반과제, 형식화과제 및 전문가과제를 구별하는것이 편리하다. 일반적으로 이 과제들을 수행하는 능력은 서로 의존되여 있다.

전문가과제에는 과학적인 분석, 공학설계 그리고 의학진단과 같은 과제들이 포함된다. 이 과제들을 수행하자면 우선 기초수학 및 론리연산과 같은 일정한 형식화과제들에 정통하여야 한다. 이 형식화과제들의 실행은 감각, 인식 그리고 주어 진 문제범위에서 언어처리와 같은 일반과제를 수행하는 능력에 의존한다. 잘되자면 형식화된 과제들은 잘 째인(명백한) 문제들에 대하여 실행되여야 한다. 사람은 문제의 범위를 리해하고 정의하기 위하여 감각 및 추리와 같은 일반기능들을 리용한다. 사람들이 감각기능을 통하여 얻게 되는 세련이 없다면 형식화된 방법들은 쓸모가 없게 된다. 간단히 말하면 전문가과제들은 일반기능을 응용하여 리해하게 되는 문제들이 적당한 공식적인 방법에 의하여 실행될것을 요구한다.

콤퓨터는 바로 계산수단이다. 콤퓨터는 매우 빠른 속도와 높은 정확도로 2진대수를 리용하여 단순한 연산을 실행할수 있도록 제작되였다. 콤퓨터는 수백만개의 단순한 연산들을 특수한 방식으로 편성하여 더 복잡한 기능들을 실행할수 있다. 한편 인간의 지능은 콤퓨터에서 복제하기 어려운 수준 높은 과제들을 자연스럽게 처리할수 있다. 콤퓨터는 인간지능의 능력을 잘 복제하지 못한다. AI연구가 이 간격을 보충하는 방법을 관찰하기에 앞서 지능의 독특한 두가지 능력 즉 일반화와 학습능력에 대하여 보기로 하자.

- **일반화.** 인간은 자기에게 제시된 개념들을 일반화할수 있고 사물현상의 구체적인 특성과 함께 본질을 인식할수 있다. 인간은 입력자극(례컨대 객체, 상태, 개념, 느낌 등)의 명확한 특징들을 매개의 구체적인 마지막세부를 기억하지 않고도 식별한다. 인간의 지능은 입력자극의 본질을 리해할수 있으므로 인간은 객체를 기억하지 않고도 학습을 통하여 개념을 리해한다. 이것은 사람이 이미 학습을 통하여 인식한 원래의 개념의 실례로부터 조금 변할수 있는 개념의 실례들을 인식하게 한다.
- **학습.** 인간은 자기의 경험으로부터 학습할수 있는 능력에서 기계와는 다르다. 만일 사람들이 오늘에 본 객체가 장방형이라는 말을 듣는다면 사람은 그것을 기억하고 래일, 다음주 그리고 다음해에도 같은 객체를 장방형으로 식별할것이다. 인간지능은 사유패턴과 개념들을 기억할수 있는 큰 기억용량을 가지고 있다. 앞으로 리용하여야 할 방식에 기초하여 정보들을 편성함으로써 인간지능은 필요할 때마다 기억된 정보를 되살릴수 있는 거대한 능력을 제공한다. 사유패턴을 기억하고 되살리는 이 능력을 학습이라고 한다.

지식의 역할

수십년간의 AI연구는 적어도 다음과 같은 하나의 론박할수 없는 주장을 론증하였다. 즉 지능은 지식을 요구한다. 지식은 인간의 감각기능을 위한 환경과 그리고 문제해결에서 공식적인 방법들을 응용하기 위한 기틀을 제공한다. 인간은 기본기능들을 반복하여 실행하는 능력은 가지고 있지만 지식이 없이는 지능을 련상케하는 방식으로 그 활동들을 편성하는 능력은 충분히 가지고 있지 못하다.

료리에서 두개의 옥파가 필요하다고 가정하자. 감각기능으로 사람은 식료품보관실에

있는 옥파 하나를 인식할수 있다. 형식화된 수학기능에 의하여 사람은 옥파가 한개밖에 없고 하나 더 필요하다는것을 판단할수 있다. 상점에 가서 옥파 하나를 사올 필요가 있다고 결심하는것은 전문가과제이다(비록 특별히 어려운 과제는 아니지만). 이 모든 기본기능은 지식에 의하여 결합된다. 사람은 이미 가지고 있는 옥파들을 찾을 장소를 알고 있다. 사람은 옥파가 몇개나 있는가를 보기 위하여 세 보아야 한다는것을 알고 있다. 사람은 몇개의 옥파가 더 필요한가를 판단하기 위하여 단순한 덜기연산을 실행하여야 한다는것을 알고 있다. 이 모든 단편적인 지식이 없다면 문제를 풀기 위하여 일반과제, 형식화과제 및 전문가과제들을 편성할수 없다.

기계는 형식화과제들을 실행하는데서는 우월하다. 수학 및 론리와 같은 과제들은 형식화적으로 정의될수 있고 콤퓨터에 의하여 거대한 속도와 정확도로 실행될수 있다. 그러나 자명하지만 기계는 앞에서 언급한 일반과제와 전문가과제들을 수행하기는 아주 어렵다. 그것은 대체로는 지식을 콤퓨터가 리해할수 있는 방식으로 표현하는것과 관련된 난점에 기인된다.

인간은 지식을 창조하고 기억하고 되살리며 응용하는 뛰여난 능력을 가지고 있다. 유감스럽게도 지식은 방대해 지고 특징을 부여하기가 어려우며 끊임없이 변화되여 가기때문에 기계로 처리하기가 어렵다. 더우기 인간의 지식은 리용방향에 따라 편성된다. 이것은 구조적인 방식으로 편성되는 콤퓨터자료와 크게 차이난다. 만일 기계가 문제들을 지능적인 방식으로 풀기를 바란다면 인간은 기계에 필수적인 지식과 그 지식을 활용하는 능력을 부여하여야 한다. 실용적으로 그 지식은 다음과 같은 일정한 특성을 가져야 한다.

- 지식은 일반화되여야 한다.
- 지식은 간단한 변경이나 수정 그리고 갱신이 가능해야 한다.
- 지식은 그것이 완전하지 못하거나 혹은 총체적으로 정확하지 못하다 해도 무수한 정황에서 리용할수 있어야 한다.
- 지식은 방대한 그자체의 지식공간을 주어 진 정황에 맞는 부분공간으로 축소할수 있어야 한다.

지식기지형체계라는 용어는 우의 조건을 만족하는 편리한 방식으로 전문지식을 표현하고 문제해결에 그것을 적용하는 수단을 제공하는 문제해결체계를 표현하기 위하여 사용되는 용어이다. 신경회로망을 리용한 패턴정합이 지식에 기초한 체계의 한 실례이다. 이 장에서는 콤퓨터침입탐지의 범위에서 신경회로망기술을 리용한 지식의 표현 및 활용에 대하여 론의한다.

패턴정합식침입탐지수법

AI기술을 침입탐지에 적용하는데서 누구나 바라는것은 인간의 수동적인 분석의 효과성을 개선하는것이다. 사람들은 탐지 및 응답과정에서의 자기의 참여를 줄이려고 하며 또한 자기가 참가하는 경우라 해도 허위경보신호의 수를 줄이려고 한다. 이것은 정의 허

위와 부의 허위의 오유률로 측정되는 침입탐지체계의 정확성을 개선하는 방법으로 달성될수 있다. 정의 허위률은 체계가 발생하는 허위경보의 퍼센트이다. 부의 허위률은 체계가 놓친 실제침입의 퍼센트이다. 매혹적인 정의 허위률을 가지는 체계를 개발하면 사람이 조사하여야 할 사고의 수를 줄일수 있다. 그러나 정의 허위률을 줄일 때에는 실제적인 침입을 꼭 탐지한다는것을 담보하는 매혹적인 부의 허위률을 유지하는데 주의를 돌려야 한다.

패턴정합은 침입탐지와 관련하여 론리적인 선택으로 된다. 침입탐지에서 가장 주요한 난점의 하나는 새로운 공격을 인식하는것이다. 이 새로운 공격은 이미 알려 진 기술의 외적인 변동이나 혹은 체계에 침투하는 완전히 새로운 방법일수도 있다. 어느 경우에나 많은 전통적인 침입탐지체계들은 그 공격을 인식하는데서 애로를 느낄것이다. 패턴정합은 일반화능력을 리용한다. 패턴정합은 새로운 입력과 알려 진 패턴사이의 정확한 특징별정합이 아니라 입력이 알려 진 패턴의 《본질》을 가지고 있는가를 판별한다. 이 수법은 두개의 실체로 하여금 외견상의 특징은 일부 다르다 해도 서로 정합되게 한다.

이 부분에서는 두개의 구체적인 AI기술에 기초한 개념적인 패턴정합침입탐지체계를 고찰한다. 신경회로망은 체계의 뇌수와 같은 역할을 하며 문제범위와 관련한 지식을 기억하고 그 지식을 침입탐지에 적용한다. 자체조직화사영은 수집된 원자료(raw data)에 대한 상관연산을 실행하여 그 자료를 신경회로망이 처리할수 있는 무리로 분해한다.

먼저 침입탐지에 관한 몇가지 기본개념들을 소개하고 우의 두가지 AI기초에 대하여 더 상세히 고찰한 다음 그것들이 지능적인 침입탐지체계구성에 어떻게 리용되는가를 보기로 하자. 여기서 론의되는 개념체계는 죠지아기술대학의 죠지아기술연구소에서 개발시험되였다.

침입탐지

침입탐지의 목적은 기관의 보안방책에 위반되는 활동을 식별하는것이다. 침입탐지문제에는 본질적으로 다음과 같은 두가지 수법 즉 오용탐지와 변칙(anomaly)탐지가 있다. 오용탐지체계들은 공격표적 즉 달갑지 않은것으로 알려 진 활동패턴을 정의한다. 이 체계들은 공격을 의미하는 표적의 존재때문에 체계활동을 감시하는데 온 시간을 소비한다. 례를 들면 IP파케트가 모든 TCP기발들이 설정된 대면부와 교차한다는것을 고찰하는 사람은 아마도 XMAS가 주사하는것을 알아 차리고 따라서 경보신호를 낼수 있다.

이 수법은 효과적일수는 있지만 여러가지 약점이 있다. 철저한 공격표적자료기지를 구축하는것은 어려우면서도 시간을 소비하는 과제이다. 더우기 알려 진 공격의 약간한 변동은 그 공격의 예정된 표적과 크게 차이날수 있고 오용탐지기가 그 사고를 총체적으로 놓치는 결과를 초래할수 있다. 사람들은 알려 진 공격을 특별히 주시하므로 오용탐지기들은 보통 표적이 자료기지에 없는 새로운 공격은 식별하기가 어렵다. 오용탐지기들은 정의 허위보다 부의 허위를 더 많이 가지고 있을 경향이 있다.

변칙탐지체계는 각이한 원리에 기초하고 있다. 변칙탐지기들은 접수할수 있는 체계활동모형을 정의하고 그 모형에 조화되지 않는 행동들은 식별한다. 변칙탐지기들은 구체적인 침입들이 무엇으로 보이는지를 알지 못하며 오히려 정상적인 행동이 무엇으로 보이

는가를 알며 정상상태로부터의 기발편차를 잠재적인 침입으로 리해한다. 례를 들어 한 회사의 쏘프트웨어기사가 한주일동안 매일 아침 7시와 9시사이에 체계에 가입하고 오후 5∼6시사이에 등록을 해제한다고 가정하자. 그리고 쏘프트웨어기사가 주말에는 체계에 절대로 가입하지 않는다고 하자. 한 기사가 월요일에 출근하여 다섯명의 쏘프트웨어기사 모두가 전날 일요일 아침 2시에 체계에 가입하였다는것을 알았다고 가정하자. 이 행동은 비정상적인 행동으로 부각되며 비합법적인 활동의 표식으로 될수 있다. 이 변칙을 식별함으로써 잠재적인 침입을 식별한다.

변칙탐지체계들은 일정한 정황속에서는 충분하지만 그 자체로는 풀기 어려운 난점도 포함하고 있다. 불량행동을 량적으로 모형화하기 어려운것과 마찬가지로 접수할만한 행동을 모형화하기도 어렵다. 변칙탐지기들은 대규모환경에서는 자주 발생하는 체계리용방식에서의 불의의 변화에 적응하기 어렵다.

이 장에서 서술되는 패턴정합침입탐지체계는 오용탐지수법에 따른다. 그 착상은 신경회로망이 입력을 일반화하고 그 입력의 외적인 변화를 인식하는 능력을 리용하는것이다. 체계는 신경회로망에 기초한 공격의 변동을 인식하여 전통적인 오용탐지기들이 발생하는 부의 허위중에서 많은것을 피하여야 한다.

일반화는 체계로 하여금 공격이 조금 변화되였지만 기본적으로는 원래것과 같다는것을 인식하게 한다. 신경회로망은 표적에 기초한 체계의 범위를 벗어 난 변화도 인식할수 있어야 한다. 더우기 일반화는 체계로 하여금 일반적으로 특수한 공격이 아닌 공격을 표시하는 조건을 인식하게 한다. 만일 총체적으로 새로운 공격들이 그 특성들을 나타낸다면 체계는 그 공격들을 이전에 본 일은 없지만 식별할수도 있다.

신경회로망

신경회로망침입탐지체계를 구축하기전에 신경회로망의 몇가지 기본개념들을 보기로 하자. 침입탐지체계의 구성에 대한 론의로 이행하면서 일부 개념들을 더 깊이 고찰하고 그 기본기능들을 확장한다.

다빈치의 지능원리들은 문제풀이에서 상사성에 주의를 돌리게 한다. 레오나르드 다빈치는 사람들이 어느날에 어떻게 새들처럼 날수 있는가를 더 잘 리해하기 위하여 새들이 나는 방법을 관찰하였다. 콤퓨터를 더 위력하고 효률적인 문제풀이기계로 발전시키기 위하여 노력하면 자연히 이미 알려 져 있는 가장 위력한 정보처리체계인 인간지능에 마음이 끌리게 된다. 련결성(connectionist)AI리론에서는 인간뇌수가 바로 감각, 추리 및 학습과 같은 과제실행을 쉽게 할수 있다고 추측한다. 그 리론에 의하면 만일 뇌수모방(수자식콤퓨터모방에 기초하는것이 아니다)에 기초한 계산모형을 구축한다면 콤퓨터는 인간지향적인 과제들의 일부를 능숙하게 실행할수 있다. 신경회로망은 그러한 련결성모형의 하나이다. 신경회로망은 뇌수의 동작을 정확히 모방하는것이 아니라 오히려 뇌수의 기능방식으로부터 령감을 유도하여 인간지능의 일부 능력을 달성하려고 한다.

신경회로망은 두개의 기본요소 즉 단순한 처리요소와 그 요소들사이의 무게 붙은 결합으로 구성된다. 신경회로망은 처리요소들이 서로 독립적으로 동작하므로 병렬도가 높은 체계이다. 결국 망조종은 망의 처리요소들에 대한 조종으로 된다. 련결성모형에서 처

리요소들사이의 무게는 체계의 지식을 표현한다.

신경회로망은 주어 진 입력이 이전 경험으로부터 학습을 통하여 알려 져 있는 패턴과 정합되는 패턴정합문제에서 특히 유용하다. 또한 신경회로망은 불완전하거나 혹은 변동되는 패턴실례들을 인식하는 근사정합을 수행하는 경향을 보여 주고 있다. 여기서 리용하는 신경회로망의 형태인 다층역전파망은 인기가 있으며 신경회로망을 리용하는 대다수의 실천응용에서 리용되고 있다고 보아 진다. 이 회로망은 패턴정합문제에 대하여 확증된 기록을 가지고 있다. 다층역전파망에 대하여서는 후에 더 구체적으로 고찰된다. 여기서는 그 망의 보다 단순한 조상인 퍼쎕트론에 중심을 둔다.

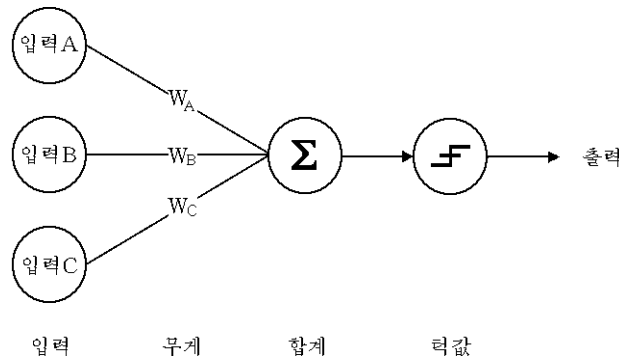



그림 36－1. 간단한 퍼쎕트론

퍼쎕트론은 가장 단순한 신경회로망이다. 퍼쎕트론은 2진값의 입력벡토르와 실수값의 무게벡토르를 가지며 두 벡토르의 벡토르적을 계산하는 망이다. 그 결과는 퍼쎕트론에 대하여 2진값출력을 발생하는 턱값함수에 적용된다(그림 36－1 참고).

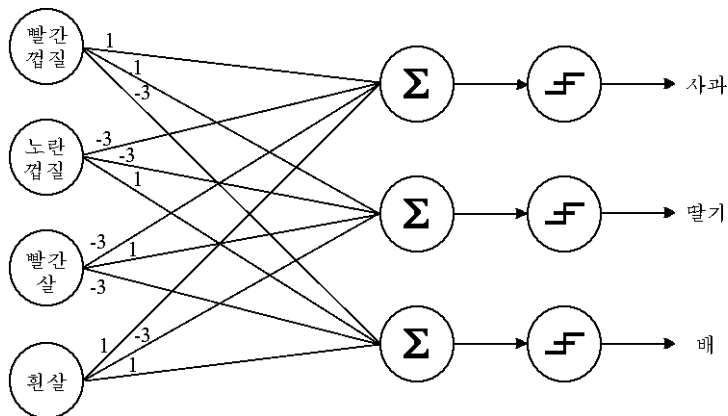



그림 36－2. 과일분류퍼쎕트론

패턴정합체계로서 이 회로망은 어떤 입력이 단일한 개념과 정합되였는가를 알수 있게 하지만 그이상의 결과는 주지 못한다. 여러개의 패턴들을 구별할수 있는 패턴정합체

계를 구성하기 위하여 다중처리요소들을 단일한 입력벡토르로 맺을수 있다. 사과와 딸기 그리고 배를 식별하는 그림 36－2의 단순한 회로망을 고찰하자. 매개 처리요소는 그에 대응하는 출력에 대한 2진값을 계산한다(단순한 퍼쎕트론의 경우와 같다).

세 원소를 가지는 출력벡토르는 입력벡토르와 정합된 패턴을 가리킨다. 례를 들어 이 회로망이 껍질은 붉은색이고 살은 흰 파일(입력벡토르 [1, 0, 0, 1])로 본다면 그 회로망은 매개의 가상처리기에서 다음의 결과들을 산생할것이다. 즉 사과 2, 딸기 –2, 배 –2. 턱값함수는 만일 입력이 정이라면 1을 산생하고 기타 경우에는 0을 산생한다. 따라서 최종적인 출력벡토르는 [1, 0, 0]이며 이것은 파일이 사과라는것을 가리킨다. 파일의 껍질이 붉은색이고 살도 붉은색이라고 가정하자(입력벡토르 [1, 0, 1, 0]). 그 합은 각각 –2, 2, –6 일것이다. 결국 출력벡토르는 [0, 1, 0]이며 이것은 파일이 딸기라는것을 가리킨다. 이 단순한 회로망은 많은 경우(배들가운데서 누런 사과를 인식하는것과 같은)에는 분명히 난점이 있지만 퍼쎕트론패턴정합의 기본개념을 례증한다.

임의의 신경회로망지식은 그 처리요소들사이의 무게로 부호화된다. 파일분류기와 같은 단순한 회로망에서는 그 무게를 수동적으로 결정하는것이 어렵지 않다. 그러나 회로망의 규모가 증가하여 복잡한 패턴들에 정합시켜야 할 경우에는 수동적인 무게결정이 무의미하게 된다. 련결성모형의 위력은 회로망이 학습한다는것이다. 다시 말하면 신경회로망은 교사 있는 학습과정을 통하여 자기의 지식을 전개한다.

패턴정합식침입탐지체계

일반적으로 침입탐지절차는 다음과 같은 5개 단계로 구성된다.

1. **원자료의 수집.** 이 실례에 대해서는 IP파케트가 리용되지만 그 원자료는 사용기록부기입내용(log entry)일수도 있고 어떤 환경에서의 활동의 임의의 다른 계량척도일수도 있다.
2. **원자료에서 자료요소추출.** 이 자료요소들은 의미를 가져야 하지만 기본적인 특징을 가지는것이여야 한다. IP파케트에 의하여 자료요소들은 원천주소와 목적주소, 규약형태, 기발들 그리고 유효자료에 대한 일부 정보들을 포함하여야 한다.
3. **선택된 자료요소들을 하나의 흔적으로 맺기.** 련관된 항목들은 총체적으로 분석될수 있는 단일한 단위로 집중될수 있다. 례를 들어 TCP대화시간내의 파케트들은 하나의 흔적으로 무리 지어 질수 있다.
4. **흔적이 공격인가를 판별하기 위한 평가.** 여기에 지식이 적용된다. 인간의 지식(혹은 체계의 지식)에 기초하여 평가되여야 할 흔적에 공격을 의미하는 특성들이 존재하는가를 판단한다.
5. **출력발생.** 이 최종단계에서 체계는 흔적에 대한 판결을 내리고 그 흔적이 공격인가 아닌가를 지적한다.

이것은 침입탐지의 일반적인 절차이며 대부분의 오용탐지기들은 류사한 방법론에 따른다. 이 절에서 고찰하는 AI식방식도 역시 그 방법론을 리용하지만 효률성을 개선할 목적으로 일부 최신기술을 적용한다. 구체적으로 체계는 자체구성사영(self–organizing map)이라고 하는 발견수법을 리용하여 자료요소로부터 흔적을 구성하며 다층역전파망(multiplayer backpropagation network)으로 알려 진 패턴정합기술을 리용하여 공격의 존재여부를 조사하기 위하여 흔적을 평가한다. 이 개념들은 후에 더 구체적으로 서술된다.

이 례증은 신경회로망에 기초한 침입탐지에 중심을 두지만 그 개념들은 다른 형식의 침입탐지에도 직접 적용될수 있다.

자료수집과 추출

침입탐지방법론의 첫번째 및 두번째 단계는 보통 현존도구들과 기술을 응용하여 달성할수 있다. IP파케트의 실례에서는 파케트를 획득하기 위하여 망엿보기장치(sniffer)나 이러저러한 대면부가 리용된다. 파케트해신기는 획득된 파케트에서 자료요소들을 해부하고 추출하는데 리용된다. 체계운영기록(system log)인 경우에는 체계의 모든 기록입구점들을 획득하기 위하여 원격운영기록봉사기가 리용되며 자료요소들을 추출하는데는 단순한 표준적인 표현분석기가 리용된다.

흔적구성

사람들의 감각기관은 많은 원천으로부터 끊임없이 많은 자료들을 받고 있다. 이 원자료들은 인간지능이 처리할수 있는 자료단위로 해부되고 결합된다. 망련결에도 류사한 현상이 있다. 망련결은 가변적인 원천, 목적지, 규약 및 선택을 가지는 파케트들을 끊임없이 받고 있다. 신경회로망을 리용하여 망통화량에서 공격패턴을 인식하자면 우선 그 자료들을 의미 있는 집합 즉 신경회로망이 처리할수 있는 자료단위로 구성하여야 한다. 이 자료단위를 **흔적**이라고 부른다.

자체구성사영(SOM)은 원래의 감각적인 입력으로부터 추출된 자료요소를 처리가 진행되는 의미 있는 큰 무리(cluster)로 변환하는 하나의 수법이다. SOM은 본질적으로 신경원형의 세포로 이루어 진 2차원격자이다. 변환함수는 입력벡토르에 존재하는 값들에 기초하여 사영되는 일정한 세포들을 려기시킨다. 그림 36－3에 보여 준것처럼 SOM은 입력들의 상관관계를 구하여 사영내에서 위상구조적인 이웃들이 입력벡토르와 일정한 기본특징들을 공유한다는것을 담보한다.

그림 36－3은 두가지 위상구조적인 이웃모임이 려기된 작은 SOM의 개념적인 표현을 보여 준다. 서로 가까운 무리들은 사영에 련관이 있는 입력이 제시될 때 려기된다. 사영되는 무리는 그 무리안의 세포들을 려기시키는 입력벡토르에 대한 지표이다. 이 그림의 사영은 두개의 무리를 보여 준다. 입력벡토르들은 론리적으로 두개의 클라스로 무리지어 진다. 이 침입탐지체계에서 매개 무리는 흔적을 표현한다.

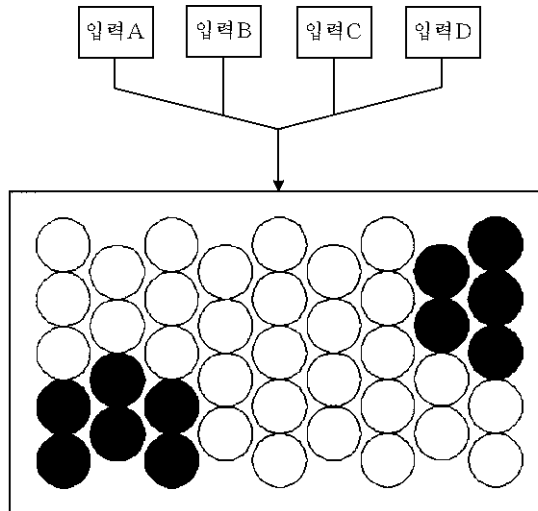



그림 36－3. 개념적인 SOM려기

SOM은 교사 없는 학습과정을 통하여 련관된 입력을 분류한다. 교사 없는 학습에서 체계는 그 무리들이 무엇과 같은가에 대한 어떠한 사전지식이 없이 자료요소들을 련관된 항목들의 무리로 구성한다. 신경회로망은 자료요소들이 어떻게 무리 지어 지는가를 자체로 결정한다. 교사 없는 학습은 흔히 교사 없는 학습과정에 앞서 입력공간의 기본특징들을 발견하기 위하여 여기에서와 같이 리용된다.

SOM학습에서 변환함수의 파라메터들은 우연값으로 초기화된다. 그러나 매개 입력벡토르는 사영에 순차적으로 제시된다. 매개 입력벡토르에 대하여 SOM은 자기의 변환함수를 적용하여 수값을 발생한다. 그 수값은 사영의 어느 세포들이 려기되여야 하는가를 결정한다. 그러면 SOM은 입력벡토르들이 얼마나 잘 무리 지어 졌는가를 측정하는 오차함수를 계산한다. 그 결과에 기초하여 SOM은 변환함수의 파라메터들을 오차함수의 크기를 감소시키도록 조절한다. 오차함수가 작다는것은 한 무리의 벡토르들사이에 강한 상관관계가 있다는것을 의미한다.

SOM은 다음으로 다음번 입력벡토르에 대하여 우에서 언급한것과 같은 연산을 반복한다. 모든 입력벡토르들이 처리되면 한 주기가 완성된다. 그 다음 SOM은 다른 주기를 실행하여 모든 입력벡토르들을 순차적으로 처리하고 그에 따라 변환함수의 파라메터들을 조절한다. 매개 무리의 벡토르들의 상관관계는 매 주기마다 개선된다. 그 상관관계가 어떤 예정된 턱값에 도달할 때까지 SOM은 매 주기실행을 계속한다. 학습과정이 끝난 후 변환함수의 파라메터들은 고정되며 체계는 연산방식으로 이행한다.

SOM의 출력은 주어 진 무리에 의한 첨수를 가지는 자료요소의 표현이다. IP통화량에 적용될 때 그 표현은 파케트들의 집합 혹은 흔적이다. 이 흔적은 패턴정합체계의 입력벡토르로 된다. 흔적 그자체를 회로망의 입력으로 리용하는 외에 사람들은 그 흔적에 대한 일부 기본통계량들(평균크기, 파케트계수, 파케트빈도수 등과 같은)을 계산하여 패턴정합체계에 제공한다.

이 체계에서 SOM은 원래의 IP파케트로부터 추출된 자료가 사영의 입력으로 적용될 때마다 출력을 발생한다. 이렇게 되면 순간적으로 포착되는 일부 흥미 있는 림시분석능력이 생긴다.

흔적평가

퍼쎕트론은 앞에서 단순한 패턴정합체계로 소개되였다. 그러나 단순한 퍼쎕트론으로 구성된 망은 주요한 제한성을 가지고 있다. 이 망들은 상대적으로 엄격한 일부 한계점들에 부담되는 일정한 형태의 입력공간에 대해서만 리용될수 있다. 그 리유는 퍼쎕트론이 단순한 개념들만을 인식할수 있다는 사실에 있다. 보다 견고한 패턴정합체계를 구성하자면 복잡한 특징을 가지는 복잡한 개념들을 인식할수 있는 능력이 필요하다. 이것은 단순한 퍼쎕트론의 확장인 다층역전파망을 리용하여 달성할수 있다.

다층회로망은 그림 36－4에 보여 준것처럼 또 하나의 처리층을 추가하는 방식으로 단순한 퍼쎕트론모형을 확장한다. 숨은 층은 복합특징들을 표현하는데 리용된다. 그 숨은 층의 매개 요소들은 학습을 통하여 단일한 복합특징을 인식할수 있다. 여러개의 숨은층을 가지는 회로망은 많은 복합특징들을 가지는 복잡한 개념들을 인식할수 있다.

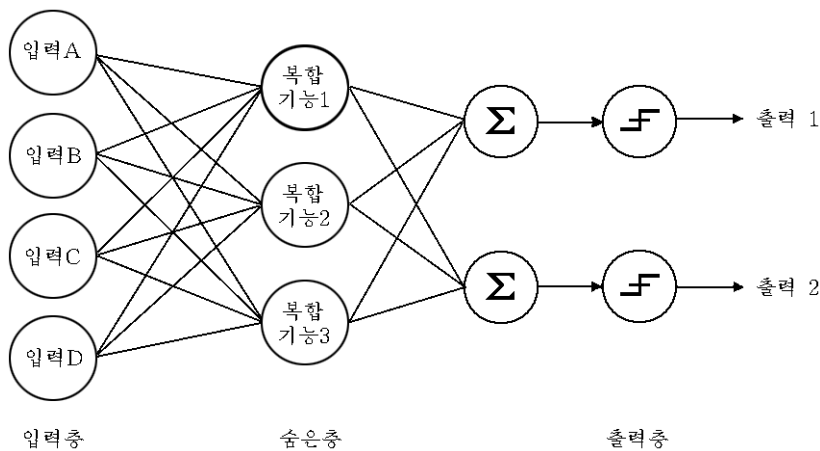



그림 36－4. 다층역전파회로망

학습. 신경회로망의 가장 흥미 있는 특성은 학습능력이다. 회로망은 주요개념들에 대한 그자체의 내부표현을 전개하여 지식을 구축한다. 신경회로망의 위력은 사람이 신경회로망에 그 개념들을 프로그람화하지 않아도 된다는데 있다. 다시 말하면 사람은 그 개념들이 무엇인가를 알지 않아도 된다. 숨은층의 요소들은 백판 즉 령으로 시작하며 회로망은 어떤 개념들이 전반적인 문제에 대한 기본열쇠인가를 결정하게 된다. 회로망은 그 개념들을 표현하기 위하여 숨은층의 처리요소들을 전개한다.

신경회로망패턴정합기는 교사 있는 학습과정을 통하여 학습한다. 교사 있는 학습에서는 일련의 훈련입력들과 그에 대응하는 정확한 출력들이 패턴정합체계에 제시된다. 이

것은 회로망이 정확한 답이 무엇이여야 하는가에 대한 개념에 기초하여 학습하게 한다. 회로망은 모든 입력패턴들에 정확히 정합되게 하는 무게를 결정한다. 만일 훈련패턴모임을 품을 들여 잘 제시한다면 회로망은 학습을 통하여 매우 높은 정확도로 패턴들을 정합시킬수 있다.

기본학습알고리듬은 다음과 같다. 회로망의 모든 무게들은 –0.1과 0.1사이에서 우연값으로 초기화된다. 매개 입력벡토르는 순차적으로 회로망에 제시된다. 입력벡토르가 제시되면 회로망은 입력층의 려기를 0과 1사이의 실수를 발생하는 려기함수에 기초하여 숨은층에로 전파한다. 이 모호결과(엄밀한 불대수의 0과 1려기와는 반대로)는 주요특징들이 입력벡토르에 존재하는 정도를 더 정확하게 반영할수 있게 한다. 다음으로 숨은층의 려기는 같은 려기함수에 의하여 출력층에로 전파된다. 이 과정을 **정방향전파**과정이라고 부르며 출력요소는 0과 1사이의 실수를 발생한다.

출력층이 일단 려기되면 계산결과와 알려 져 있는 정확한 결과사이의 오차함수를 계산할수 있다. 그 오차에 기초하여 회로망의 무게들은 오차함수의 크기가 감소하도록 조절되며 회로망은 다음번 입력에로 이행한다. 무게조절과정을 **역전파**라고 부른다.

모든 입력벡토르들이 처리되면 한 주기가 끝난다. 회로망은 오차함수의 크기가 허용수준으로 감소될 때까지 주기를 반복한다. 일단 그 과정이 완결되면 회로망은 학습을 통하여 회로망에 제시된 입력벡토르에서 패턴들의 존재를 인식한다. 모든 신경회로망학습과 마찬가지로 신경회로망의 정확성은 단지 학습과정에 표본패턴들에 대하여 획득하는 경험에 의존한다. 결국 충분한 훈련공간을 선택하는것이 관건적이다.

침입탐지체계를 숙련시킬 때 체계는 허용된 회로망통화량과 이미 알고 있는 모든 공격들을 체계적으로 받는다. 만일 체계가 공격통화량에 대해서만 훈련된다면 회로망은 학습을 통하여 공격으로 간주하는 모든것을 인식한다. 만일 체계가 허용된 통화량에 대해서만 훈련된다면 그 역이 성립한다. 효률적인 학습을 담보하자면 두 경우사이의 균형이 필요하다.

연산. 일단 학습과정이 완성되면 신경회로망의 무게들은 고정되고 체계는 연산준비가 완료된다. 연산하는 동안에 입력벡토르(SOM무리짓기사영의 흔적출력)는 다층역전파망의 입력마디점에 적재된다. 회로망은 학습할 때 리용한 같은 려기함수에 기초하여 입력층의 려기를 숨은 층에로 전파한다. 다음 숨은 층의 려기는 학습과정에서와 꼭 마찬가지로 출력층에 전파된다. 출력층이 일단 려기되면 결과가 발생된다.

그 결과는 0과 1사이의 실수값이므로 사람은 그 결과만이 아니라 려기의 크기에 기초하여 행동을 취할수 있다. 례를 들어 0.9이상의 임의의 려기를 즉시적인 응답을 요구하는 공격으로 통보하고 그리고 0.75～0.89의 임의의 려기를 더 고찰해 보아야 할 흥미 있는 사건으로 통보하는 턱값함수를 리용할수 있다.

가동하는 체계

체계가 들어 오는 통화량을 평가하여 공격패턴의 존재를 어떻게 판별하는가를 관찰하자. 그림 36－5는 총체적인 체계의 개념적인 례증이다.

IP파케트를 획득하는데 엿보기도구(sniffer)가 리용된다. 그 패기트는 해신되고 주요한 자료요소들은 추출된다. 이 자료요소들은 하나의 단위로 묶어 져 자체구성사영의 입력으로 작용한다. 사영은 그 파케트와 주요한 특성들을 공유하는 다른 파케트를 함께 무리 지어 놓으며 새로운 파케트와 그것의 위상구조적인 이웃들을 포함하는 흔적을 출력한다. 그 흔적은 그 자료에 대하여 출력층에로 려기를 전파하는 신경회로망의 입력으로 작용한다. 출력려기에 기초하여 흔적은 공격과 공격이 아닌 흥미 있는 사건으로 식별된다.

포구스캔탐지

공격자들은 흔히 실제공격목표를 식별하기 위하여 포구스캔(port scan)을 진행한다. 그것은 어떠한 직접적인 손상도 주지 않지만 사람들은 포구스캔을 그의 악성적인 의도로 하여 공격으로 취급한다. 직접적인 포구스캔은 탐지하기가 비교적 쉽다. 같은 원천주소와 같은 목적주소 그리고 매개 목적포구가 스캔된다. 그러나 만일 공격자가 례컨대 하나의 포구를 2～3시간마다 스캔하는 방법으로 여러번 스캔을 반복한다면 침입탐지체계를 피할수도 있다.

자료요소들로부터 흔적을 구성하는 방법은 독특한 림시분석능력을 제공한다. 패케트들이 무리에 추가될 때 그 무리는 흔적을 발생한다. 만약 무리들이 충분한 시간동안 SOM에 머무르게 된다면 보충적인 파케트들은 비록 그것들이 긴 시간동안 공간적으로 퍼지지만 수신될 때에는 흔적에 추가될것이다. 이것은 긴 시간에 걸쳐 들어 오는 파케트들의 상관관계를 제공하여 침입탐지체계를 피하려는 느린 스캔수법을 적발하게 한다. SOM은 시간경과카메라의 역할을 하여 시간별로 널려 있는 사건들에 대하여 단일한 흔적으로 상관관계를 맺게 한다.

SYN범람탐지

SYN범람공격은 최근년간 특별히 통용되는 봉사거부공격으로서 협동공격과정의 한 부분으로 흔히 리용된다. TCP–SYN파케트들을 하나의 견본으로 포함하는 두개의 류사한 흔적을 리용하여 이 체계가 실제의 SYN범람공격과 실제로 매우 정상적인 Web통화량인 표면상의 SYN범람을 다 어떻게 인식하는가에 대하여 더 잘 리해할수 있다.

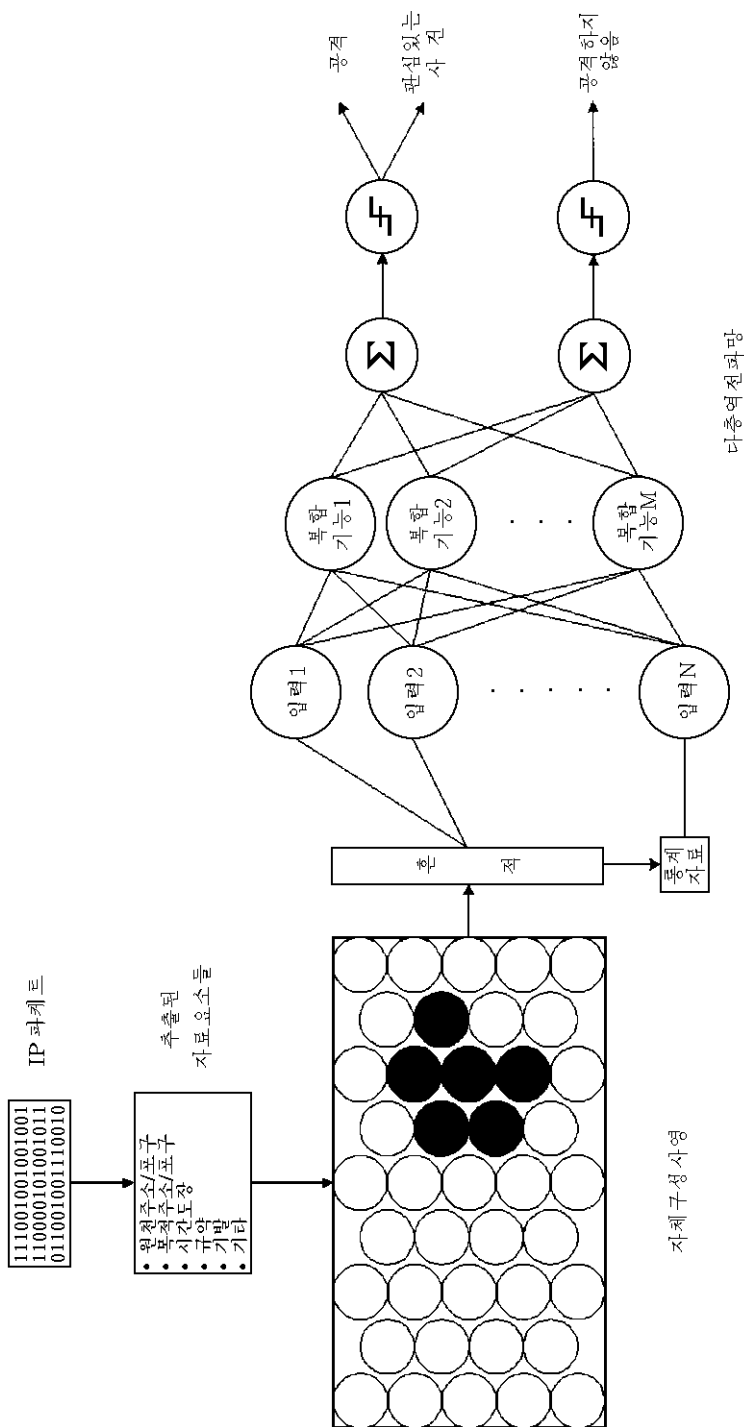



그림 36—5. 패턴정합침입검출체계구성의 개념도

표 36－1　　SYN파케트

마 당	값
시간도장	0.9 : 30 : 29 : 4257
원천주소/포구	공격자 : 320
목적주소/포구	봉사기 : 23/TCP(Telnet)
기발	S(TCP–SYN)
순서번호	1094689872
ACK번호	1094689872

표 36－1에 레증된 파케트를 고찰하자. 이것은 봉사기와의 Telnet련결의 첫 파케트인 SYN파케트이다. 그 파케트들중 여덟개 혹은 아홉개가 1초 혹은 2초간격으로 보여 지며 그 파케트들은 다음의 사항을 가진다고 가정하자.

- 같은 목적주소
- 23/TCP(Telnet)의 목적포구
- 원천포구가 증가하는 같은 원천주소
- 증가하는 순서번호와 ACK번호들
- 같은 TCP기발들,구체적으로 TCP–SYN

SOM은 파케트들이 서로 련관이 있다는것을 인식하며 그것들을 하나의 흔적에 함께 무리 지어 놓는다. 류사한 파케트가 접수될 때마다 SOM은 그것을 무리에 추가하고 신경회로망에 의하여 평가되도록 갱신된 흔적을 출력한다. 상기할것은 흔적 그자체와 흔적에 대한 몇가지 기본통계량들이 신경회로망의 입력으로 작용한다는것이다. 그 활동의 첫 2∼3μs에서 신경회로망은 SYN파케트의 빈도수가 높지만 파케트계수는 상대적으로 낮다는것을 볼수 있다. 학습하는 동안에 신경회로망은 우에서 언급한 특성과 련관시킬 때 SYN범람공격을 구성하는 파케트계수 및 파케트빈도수의 결합관계를 학습한다. 결국 SOM이 더욱 더 많은 파케트들을 무리 지어 놓을 때 우에서 언급한 모든 특성들이 최종흔적에 계속 존재하여 파케트계수 및 빈도수통계량은 증가한다. 그러면 흔적패턴은 SYN범람공격의 패턴과 정합되기 시작한다(숙련하는 동안에 신경회로망이 학습하는 내부표현에 의하여 정의되는). 턱값에 도달되면 신경회로망은 공격을 의미하는 출력벡토르를 발생한다.

신경회로망은 학습을 통하여 실제적인 SYN범람공격에 대한 훈련에 의하여 우의 패턴을 공격과 일치시키는 흔적을 인식한다. 그러면 다음의 특성을 나타내는 흔적을 발견하였다면 어떤 일이 생기는가.

- 같은 목적주소
- 목적포구 135/TCP(Net BIOS)
- 가변적인 원천주소 및 포구
- 같은 TCP기발들, 구체적으로 TCP–SYN.

원천주소와 포구가 변한다 해도 신경회로망은 여전히 이 공격을 SYN범람공격으로 인식할수 있다. 명심할것은 체계가 그 씨나리오에 대하여서는 명시적으로 훈련되지 않았다는것이다.

벡토르의 벡토르적연산은 신경회로망내에서 마디점려기함수를 계산하는데 리용된다. 만일 원래 흔적의 세번째 특징이 제시된다면 입력벡토르의 대응하는 요소는 0으로 되며 벡토르적연산의 결과는 감소된다. 그 감소는 SYN범람공격의 총체적인 묘사에서 그 특징의 중요성에 비례한다. 그 세번째 특징은 공격의 가장 지배적인 특징은 아니므로 그 감소는 상대적으로 작다. 만일 흔적의 기타 모든 사항들이 변하지 않는다면 그 감소는 신경회로망이 그 공격을 놓칠수 있게 하는데 충분할수도 있다.

그러나 더 많은 파케트들이 접수될 때 파케트계수는 증가할것이며 입력벡토르의 그 요소를 증가시킨다. 이것은 벡토르적연산의 결과를 증가시킨다. 그 증가는 SYN범람특징으로서의 《파케트결수》의 우세정도에 비례한다. 그 특징은 SYN범람의 묘사에서 매우 중요하므로 그 증가는 상대적으로 크며 다른 특징의 제거로 초래되는 감소를 보상하는데 충분하다. 이것은 려기함수가 공격경보신호를 내는 턱값이상으로 증가하게 한다.

이제 원래 SYN범람실례로부터 약간 변경된 또 하나의 파케트를 고찰하자(표 36－2 참고). 그것은 봉사기와의 HTTP접속의 첫 파케트인 SYN파케트이다. 그것들 가운데서 여덟개 혹은 아홉개의 파케트들이 1초 혹은 2초간격으로 보이며 그 파케트들은 다음의 사항을 가진다고 가정하자.

- 같은 목적주소
- 목적포구 80(HTTP)
- 원천포구가 증가하는 같은 원천주소
- 증가하는 순서번호와 ACK번호
- 같은 TCP기발, 구체적으로 TCP–SYN

앞의 실례에서와 마찬가지로 SOM은 그 파케트들이 서로 련관이 있다는것을 인식하고 그것들을 하나의 흔적에 무리 지어 놓는다. 그러나 흔적이 회로망에 제시되면 그것이 SYN범람패턴과 비슷해 지기 시작해도 그것은 공격신호로 되지 않는다. 이 실례와 앞의 실례사이의 차이는 목적포구/봉사이다. HTTP의 특성으로 인하여 많은 SYN파케트들을 이와 같이 순차적으로 보는것이 정상이다. 신경회로망이 학습하는 동안에 허용된(즉 비공격) 통화량의 표본들로서 HTTP접속을 신경회로망에 제공하였다고 가정하면 신경회로망은 그 차이를 인식하고 그 활동에 대하여 SYN범람으로 경보신호를 내는것을 취소할것이다. 신경회로망안에서는 일반적인 SYN범람패턴에 대한 이 례외가 목적포구 80/TCP에 대

응하는 입력마디점으로부터의 큰 부(–)의 무게값으로 표현된다(혹은 다른 봉사는 25/TCP 혹은 443/TCP와 같은 정의 허위 SYN범람경보신호를 낼수도 있다). 입력마디점이 능동일 때 접속은 신경회로망안에서 SYN범람려기에 기여하는 다른 입력특징들을 모두 강하게 억제한다. 그러므로 목적포구는 회로망이 일반적인 SYN범람패턴에 대한 이 례외를 인식하게 된다.

표 36-2　　　SYN파케트

마 당	값
시간도장	0.9 : 30 : 29 : 4527
원천주소/포구	공격자 : 320
목적주소/포구	봉사기 : 80/TCP(HTTP)
기발	S(TCP–SYN)
순서번호	1094689872
ACK번호	1094689872

개 념 확 장

개념모형은 여러가지 방법으로 확장될수 있다. 여기서는 그 몇가지 가능성을 고찰한다.

체계는 흔적이 공격인가 아닌가에 대한 판결만이 아니라 공격이 어떤 종류로 나타나는가에 대한 일부 표시까지도 넘겨 주도록 확장하는것이 더 좋다. 이 수법의 하나의 결함은 훈련자료에 상당한 량의 추가정보를 제공해야 한다는것이다. 이것은 공격훈련자료에 대한 정보를 회로망에 제공할 필요가 거의 없다는 우점을 해소한다.

또하나의 확장은 련속인 학습모형의 응용과 관련된다. 회로망의 초기학습주기가 끝난 다음에도 학습과정을 중단하는것이 아니라 련속하면 회로망은 그것의 실지 경험에 기초하여 지식표현을 주기적으로 조절하게 된다. 이 수법의 잠재적인 목적은 체계가 환경의 변화에 적응하고 그 환경변화를 학습하도록 하는것이다.

SOM구조와 관련한 난점의 하나는 들어 오는 파케트가 그 흔적과 함께 평가될수 있도록 어떤 무리에 속해야 한다는것이다. 그러나 만일 SOM이 들어 온 파케트를 잘못 분류한다면 침입탐지능력이 떨어 질수도 있다. 회로망의 파케트는 오직 하나의 흔적에만 속하지만 더 많은 정보가 입수될 때까지는 여러개의 흔적에 속할수도 있다. SOM의 확장은 사영이 주어 진 파케트의 복사본을 여러개의 무리에 배치 하게 한다. SOM은 하나의 파케트를 여러개의 흔적에 맞추어 어느것이 최적일치인가를 판별해 볼수 있는 가능성을 가진다. 이로부터 흔적구성도식에 고장허용준위가 도입된다.

난점과 제한성

이 개념체계의 구성을 론의하면서 침입탐지와 관련한 우점을 언급하였다. 그러나 이 수법에 약점이 없지는 않다.

잘못된 학습

신경회로망은 학습하는 동안에 상당한 정도로 공개된다. 신경회로망이 학습을 통하여 공격과 허용된 행동을 구별할 때 공격자는 신경회로망을 통하여 어떤 뒤문(back door)을 구축할 기회를 얻게 된다. 신경회로망은 공격과 허용된 활동에 대하여 다 훈련된다는것을 상기하자. 만일 공격과 같은 행동에 대하여 구체적으로 기발신호를 설정하지 않는다면 체계는 그 활동을 허용된 활동으로 인식하게 하는 어떤 내부지식구조를 생성할것이다. SYN범람규칙에 대한 HTTP례외는 좋은 실례이다. 신경회로망은 《만일 내가 흔적에서 일정한 특성들을 발견한다면 그것은 공격인데 그것이 포구 80/TCP에 대한것이 아니라면 그것은 공격이 아니다》라고 학습한다. 신경회로망은 허용된 HTTP접속들에 훈련자료가 삽입되였기때문에 그 례외를 학습하였다. 만일 공격자가 SYN범람공격을 자기의 회로망으로부터 훈련자료에 은밀히 삽입할수 있다면 회로망은 또 다른 례외를 학습할수 있다. 회로망은 이번에는 《만일 내가 흔적에서 일정한 특성들을 발견하였는데 그것이 홈페지 attacker.net로부터 온것이 아니라면 그것은 공격이다. 》라고 학습한다. 공격자는 훈련자료를 부식시켜 신경회로망이 자기의 공격을 알지 못하게 함으로써 침입탐지체계를 피한다.

다음과 같은 철학적인 문제를 고찰하자. 신경망은 인간지능으로부터 령감을 이끌어내므로 그 모형의 제한성을 자기의 체계안에 끌어 넣을 가능성을 가진다. 례를 들면 인간은 일정한 형태의 감각입력에 대하여서는 시간이 지남에 따라 반응하지 않게 될수 있다. 사람들은 주위세계에 관한 자기의 지식을 끊임없이 갱신한다. 만일 개념이 조금 변화된다면 사람들은 그 변화를 반영하도록 자기의 지식을 갱신한다. 그 작은 변화의 축적효과는 오랜 시간범위에서 보면 극적일수 있다. 텔레비죤에서 방영되는 폭력프로에 대한 무반응이 이에 대한 좋은 실례이다. 련속학습모형들은 시간이 지남에 따라 신경회로망의 지식을 점차적으로 변화시킨다. 품을 들여 완성한 활동으로 공격자는 이 개념체계안에서의 지식변화에 기여할수 있으며 회로망이 일정한 공격을 알수 없게 할수 있다. 시간이 지남에 따라 공격자는 그 기술을 리용하여 체계에 파구를 낼수 있다. 이것은 수감자가 숟가락으로 감옥안에서 땅굴을 파는것과 류사하다.

신경회로망과학

신경회로망의 련속학습모형에는 그에 고유한 여러가지 난점이 있다. 련속학습회로망들은 일정한 입력으로부터 그에 대응하는 출력까지의 명시적인 사영을 학습한다는것이 알려 져 있다. 이것은 효과상으로는 기억과정이며 일반화능력을 해소한다. 그것을 막는

한가지 방법은 일단 일정한 성능수준에 도달되면 학습을 중지하는것이다. 또 하나의 방법은 체계에 충분한 잡음을 끌어 들여 기억과정을 막는것인데 회로망을 혼란시킬 정도로 많이 끌어 들여서는 안된다. 끝으로 복잡한 특징들을 기억할수 있는 숨은층의 요소수를 줄일수 있다. 이것은 회로망이 복잡한 특징들의 더 간결한 내부표현을 학습하도록 강요하는 계산상의 난관을 초래하며 회로망의 매개의 입력/출력결합에 대한 명시적인 사영을 만들지 못하게 한다. 즉 좋기는 하되 지나치게 좋지는 않은 신경회로망이 필요하다.

신경회로망학습에서의 수학적처리와 관련하여 그에 고유한 여러가지 난점들이 있다. 복잡한 신경회로망은 흔히 학습속도가 느리다는 비평을 받는다. 훈련공간의 크기는 회로망의 크기보다 여러 자리수나 더 커야 한다. 이것은 견고한 회로망에 매우 많은 훈련표본들을 제시할것을 요구한다. 학습과정은 정의에 의하여 반복적인 과정이므로 학습은 느릴수 있다. 연구사들은 알고리듬이 자연스럽게 여러번 반복되여 좋은 학습방향에서 안착되게 하며 그 방향으로 빨리 전진하게 하는 가속수법을 개발하였다. 이것은 신경회로망의 학습속도를 상당한 정도로 개선하기는 하였지만 학습과정은 여전히 느리다.

그리고 학습알고리듬은 오차함수를 대역최소값이 아닌 여러개의 국부최소값중의 하나로 가게 하는 방향을 취할수 있다. 이것은 패턴정합기를 부정확하게 하며 언제 그것이 발생하는가 하는데 대한 판단은 직관적으로 리해할수 없다. 실천적으로 이런 일은 드물게 생긴다. 그것은 부분적으로는 대부분의 견고한 신경망에 존재하는 고차원무게공간에 의하여 제공되는 자유도가 높다는데 기인된다. 그러나 이것은 알고 있어야 할 실지문제점이다.

실제적가능성

개념–증명원형(prototype)이 실험실로부터 상업적인 상품으로 얼마나 잘 확대되는가 하는것은 아직까지 명백치 않다. AI의 실제적가능성에 대한 많은 론평들은 인공지능체계들이 가동한다고 해도 체계의 가동을 유지하자면 전임콤퓨터과학자가 있어야 한다고 주장하고 있다. 이 분야의 과학연구는 지난 10년내에 많이 발전하였고 많은것들이 상업적체계에 응용되기 시작하였다. AI에 기초한 침입탐지가 주류기술로 되는가 하는것은 두고 보아야 할 일이다. 과학적으로는 그 전망이 크다는것이 론증되고 있으며 따라서 그것을 비현실적인것으로 제쳐 놓는것은 현명하지 못할수도 있다. 그러나 인공지능은 만병통치약이 아니며 기술발전으로부터 끊임없이 제기되는 보안문제에 대하여 응당한 주의를 돌려야 한다.

결 론

실천공동체로서의 인간의 실천적경험은 보안이 어려운 문제라는것을 여러번 시인하였다. 보안문제가 명백한 경우는 매우 드물며 거의 언제나 그 사이에는 넓은 회색스펙트르(불명확성)가 있다. 인간은 그 회색그림자속에서도 잘 처리할수 있지만 콤퓨터는

결정론적인 기계이며 그런 능력을 쉽게 갖추지는 못한다. 인공지능연구의 기본목적은 콤퓨터로 하여금 현재는 인간에게 보다 적합한 주관적인 문제들을 더 잘 풀수 있게 하는것이다.

침입탐지가 그러한 과제의 하나이다. 전통적인 침입탐지수법들은 수자식계산례에 기초하고 있다. 그 수법들은 콤퓨터의 특이점 즉 객관적인 연산을 빠르고 정확하게 실행하는 특징을 리용한다. 그러나 그 수법들은 고유한 제한성을 가지고 있다. 침입탐지는 모호하며 주관적인 과제이다. 수자식콤퓨터를 리용할 때 어느것이 침입으로 되는가를 완전히 정의하는것은 불가능하지는 않지만 어려운 일이다.

이 장에서는 인간의 두뇌모방에 기초한 침입탐지수법, 구체적으로는 자체구성사영(SOM)으로 알려 진 자료발견기술을 고찰하였다. SOM은 입력공간의 파케트들을 침입을 분석할수 있는 의미 있는 흔적들로 서로 상관시킨다. 신경회로망패턴정합기는 흔적들에 침입활동이 존재하는가를 분석한다. 이 두 기술은 인간의 사유를 모방한 방식으로 침입을 탐지하는 개념체계에서 결합된다.

이 장에서 고찰된 개념체계들은 SYN범람실례를 통하여 관찰된것처럼 부의 허위오유률과 정의 허위오유률을 명백히 개선한다. 인간의 두뇌를 모방한 체계들은 패턴정합침입탐지기로서 전망이 기대된다. 아마도 AI에 관한 연구가 심화됨에 따라 지능적인 침입분석체계는 실험실단계를 벗어나 침입분석체계의 주류로 이행하게 될것이다.

참 고 문 헌

1. Northcutt, Stephen, *Network Intrusion Detection: An Analyst's Handbook.* Indianapolis: New Riders Publishing, 1999.
2. Rich, Elaine and Knight, Kevin, *Artificial Intelligence,* 2nd edition. New York: McGraw-Hill, 1983.
3. Cannady, James and Mahaffey, James, "The Application of Artificial Neural Networks to Misuse Detection: Initial Results."
4. Frank, Jeremy, "Artificial Intelligence and Intrusion Detection: Current and Future Directions," 1994.
5. Endler, David, "Intrusion Detection: Applying Machine Learning to Solaris Audit Data."

제37장. 전자상업거래환경의 검토

츄리스 해어

인터네트접근의 침투와 일부 상점을 통한 거래가 직결실행에로 이행함에 따라 전자상업거래분야에서 안정성 및 보안에 대한 요구는 점점 높아 지고 있다. 많은 성공적인 전자상업거래싸이트중의 하나인 E*Trade는 자기의 직결방식에 완전히 의존하여 기업을 유지한다. 목적과 무관계한 지출은 잠재적으로 수백만딸라의 손해를 줄수 있다. 레를 들어 2001년 초에 있은 Yahoo와 CNN에 대한 분산형봉사거부(DDoS)공격을 고찰하자. 그 공격을 저지시키는 방법이 일단 발견되기는 하였지만 수익손실외에도 체계를 재정비하는데 수천딸라가 소비되였다. 이 론문은 전자상업거래의 보안 및 신뢰성을 평가하는 방법을 설명한다. 위험평가(risk assessment)와 관련된 저자의 경험에 의하면 보안, 신뢰성 그리고 Web감각 즉 사용상의 편리성은 전자상업거래의 지속적인 성공을 위하여 관건적인것으로 인정될수 있다. 여기서 설명하는 수법들은 임의의 전자상업거래 Web싸이트소유자, 관리자 혹은 재정검사원들이 기본위험령역의 일부를 식별하고 보안하는데 도움이 될수 있다.

전자상업거래의 하부구조를 조종할수 있는가

전자상업거래환경을 개발하고 실현하는데서 가장 중요한 난점은 그 환경전체를 고착시키는것이다. 성공은 목적한 결과를 달성하기 위하여 공정과 기술, 실현을 밀접히 결합시키는데 의존한다. 최종목표의 달성은 종합적인 전략, 법적문제들과 수출문제에 관한 리해, 리용하고 있는 공정들은 물론 리용하는 기술에도 의존한다. 생각해 본후에가 아니라 우선적으로 신뢰성과 무결성 그리고 리용성 있는 환경을 구상해야 한다.

전 략

기술의 파동과 문제처리방법들에 사로잡히지 말아야 한다. 기술은 전체적인 난문제의 한 부분일뿐이다. 인간은 이미 수동적으로 운영되는 공정을 보충하여 더 넓은 시장을 개척하기 위하여 기술을 도입한다. 운영형편에 따라 기술적요구가 제기되며 또 그것은 필요한 체계의 총체적인 개발에 영향을 미친다. 계획의 실현도 흔히 기술에서의 변화보다도 오히려 기업의 변화와 법률상요구의 변화에 의한 영향을 더 받는다.

전략은 효률적인 전자상업거래실현의 기본열쇠이다. 한 회사에 종사하는 사람들은 자기들의 계획화활동과 개발활동을 전개하는데 리용할수 있는 식견이 있어야 한다. 그 식견은 상급경영자들이 내세우고 있고 또한 성공을 계량하는 기초로 되는 목표를 판단하게 한다. 전략이 없다면 회사자체와 회사의 직원들, 회사주주들 그리고 소비자들이 회사가 무엇을 달성했는가를 판단할수 없게 될것이다.

전략은 또한 회사가 작성하는 기업결정서에 기초하여야 한다. 소비자가 봉사를 받는

데 리용하는 매체에 관계없이 동료와의 거래에서 일관성을 보장하자면 현존 공동방책들이 재검토되고 보충되여야 한다.

기술은 희망을 실현하는 방법일따름이다

전자상업거래전략을 작성하는 팀은 그 전략을 실현하기 위한 목표를 정립한다. 그 목표는 연구계획과 경영활동으로 전환할수 있어야 한다. 전자상업거래전략작성에서 고려하여야 할 사항은 다음과 같다.

- 전자상업거래에로 이행하여 무엇을 달성하려고 하는가.
- 전자상업거래전략이 현존 회사전략과 얼마나 밀접한 련관성을 가지는가.
- 현존 회사기업공정중 어떤 공정들이 통합되여야 하는가.

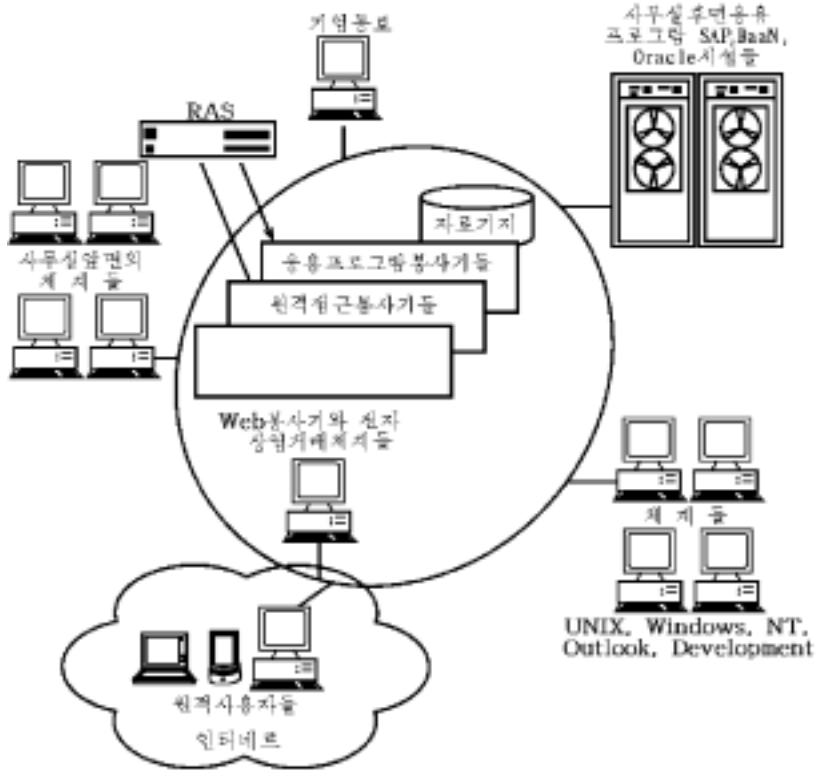



그림 37－1. 전자상업거래체계의 하부구조

- 누가 봉사를 받으려고 하는가, 기업 대 기업인가 기업 대 소비자인가 또는 둘다 인가.
- 누가 제공되는 봉사를 받으려고 하는가.
- 소비자들이 제공받고 싶어하는것은 무엇인가

이 질문들에 대한 완벽하고 철저한 해답이 나와야 비로소 그것을 실현하는 기술적해결책을 찾을수 있게 된다. 그림 37－1에 보여 준것처럼 기술적인 해결책은 복잡하며 많은 요소들을 포함한다. 기술실현과 관련한 개별적인 요소들을 선정하기전에 먼저 기업공정들에서 매개 요소들의 호상작용을 리해하여야 한다.

법률상문제

대부분의 회사들에 있어서 그것들이 상주하고 있는 나라나 거래를 가지고 있는 나라들의 법을 정확히 지키는것도 난문제의 하나이다. 법의 종류에는 지역법, 주법, 국가법, 국제법 등이 있다. 추가적인 규정들은 업계별로도 있고 공개매매된 회사인 경우에도 추가적인 규정들이 있다. 그러나 전자적방법으로 기업을 운영하는 경우 새로운 난문제들이 제기된다.

사적비밀

소비자들은 자기정보의 사적비밀보장에 관심을 가지며 한편 회사들은 소비자들이 회사에 제공하거나 혹은 회사가 그들과 공유하고 있는 정보의 사적비밀을 보장하는데 관심을 가진다. 정보의 사적비밀보장과 관련한 세계의 각이한 지역에서의 법률적요구를 제쳐놓고 본다면 기업이 사적비밀을 통제하지 못한다면 신용기업으로 되지 못할것이다. 만일 소비자들이 회사가 그것을 고려하지 않는다는것을 안다면 그들은 회사와 전자거래를 하지 않을것이다.

사적비밀문제는 회사나 기관에 몇가지 실질적인 난문제를 제기한다. 례를 들어 1999년에 유럽동맹(EU)은 정보의 사적비밀과 보호에 관한 규범을 발효시켰다. EU는 류사한 사적비밀보장규범을 실행하지 않는 회사나 나라들과는 거래하지 않을것이라고 발표하였다. 그러므로 매 회사는 자기의 사적비밀보장방책을 구체적으로 발표하여야 한다. 이것은 소비자의 정보보호에 관한 기관측의 공약이 필요하다는것을 말해 준다.

사적비밀문제를 해결한다는것은 그것을 기술적으로 실현하는 사람들이 암호, 수자식서명(digital signature) 그리고 수자식인증서(digital certificate)와 같은 단어들을 사용한다는것을 의미한다. 이것들은 사적비밀에 리용되는 기술적인 요소들이며 사용자들이 전자업무싸이트를 통하여 받거나 보내는 정보를 더 잘 보호할수 있게 한다.

그림 37－2에 보여 준것처럼 Mastercard사와 VISA사가 안전전자업무처리(SET)규약을 개발하게 된것은 소비자의 상품구입관습정보에 관한 사적비밀보장문제와 관련된다.

모든 업무처리(transaction)는 정보전송이나 비법접근에 의하여 중요한 기업정보가 손실되지 않도록 안전하게 진행되여야 한다. 이런것들을 잘 타산하여 전략에 반영해야 한다. 그렇게 하여야 불완전하게 실현된 공정이나 기술에 의한 정보손실과 성능의 감소 혹은 신뢰성의 위험을 완화시킬수 있다.

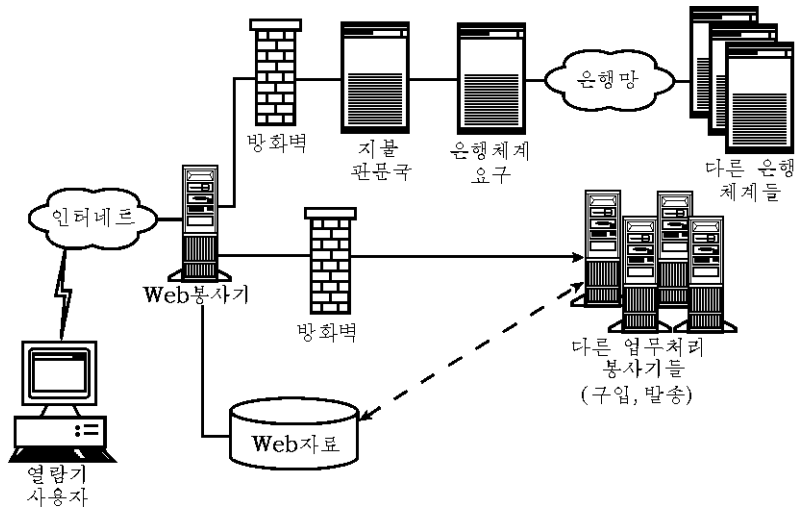



그림 37－2. 표본SET업무처리환경

수 출 통 제

수출통제는 정부에 의하여 진행되며 위험하거나 국가적리익에 맞지 않는 나라들에로의 수출은 제한된다. 대부분의 나라들이 이런 방식을 적용하고 있으며 암호기술과 같은 일부 경우에는 그 항목의 수입을 막는 나라들이 있다.

수출통제법을 잘 지킬것을 강력히 충고한다. 그것을 어긴 경우에 대한 처벌은 나라나 수출항목에 따라 매우 엄격할수 있다. 최근년간 (구체적으로는 암호를 포함한) 일부 수출규정들이 변화되였다. 나라들마다 자기의 생산업체들의 세계시장경쟁력을 높이기 위한 노력의 일환으로 암호수입/수출규정들을 고치고 있다.

전자상업거래의 하부구조를 구축할 때에는 수입/수출법을 검토하는것이 중요하다. 그 규정들이 적용되는 정보나 기술이 있을수 있고 그것은 봉사와 생산품을 받는 사람들에게 영향을 미칠수도 있다.

법 률

많은 회사들에 있어서 법작성은 주요한 분야이다. 법률에는 사적비밀보장문제를 어떻게 처리하며 기업을 일반적으로 어떻게 운영하는가를 통제하는 다양한 법률이 있다. 그 법률의 많은것들은 전자기업에만 국한되지 않는다. 인터네트망과 인터네트규정은 지적소유권으로부터 싸이버정착(cyber–squatting: 돈벌이를 목적으로 URL을 미리 등록하는 것)에 이르기까지 모든것에 해당된다.

제기되는 문제가 다양하고 법조항이 복잡하므로 자격 있는 변호사의 도움을 받을것

을 권고한다. 변호사의 도움으로 전자기업을 활성화하는 능력에 대한 법의 영향을 세심하게 고려하여야 한다.

법의 다양성을 고려할 때 관심을 두어야 할 일부 문제들을 보면 다음과 같다.

- 전자상업거래에 적용할수 있는 국가법과 국제법에는 어떤것들이 있는가.
- 법률준수는 어떻게 담보되는가.
- 어떤 나라들에서 기업들이 전자상업거래를 할수 없게 금지되는가.
- 전자적으로 효력이 발생될수 있는 상품공급관련협정과 계약들이 있는가.
- 기업이 수자식서명을 지원하는가 그리고 그것들이 기업관할권내에서 법적구속력을 가지게 되는가.
- 국내 및 국제적으로 의견상이를 어떻게 해결하는가.
- 전자상업거래의 하부구조를 통하여 리용하기전에 수출허가를 요구하는 기술이나 정보가 있는가.

개발과제관리

전략이 규정되면 회사팀은 뒤이어 관리활동을 규정하며 하부구조를 실제적으로 개발하고 실현한다. 그러나 개발과제관리(project management)는 모든 사람들이 하여야 할 일과 그 일정계획 그리고 예산량을 알도록 하는 방향으로 지향된다.

회사팀이 개발과제관리가 없이 전자상업거래봉사를 실현하게 한다면 많은 실수를 범할수 있다. 개발과제가 어디에 있는가를 판단하기는 어렵지만 그 개발과제가 언제 완수되며 그 개발과제에 얼마만한 액수가 지출되는가를 판단하기는 더욱 어렵다.

개발과제관리는 개발과제를 규정하고 그 계획이 기업의 요구조건을 만족시킨다는것을 담보하며 예산의 초과지출이 없이 제때에 완수되도록 필요한 통제기능들을 제공한다. 개발과제관리전략은 그 개발과제를 완수하는데 필요한 과제들을 규정하는데서 관건적이다. 개발과제계획은 누가 그 개발과제와 그와 관련되는 부분개발과제들의 주최인가 그리고 사용자들이 전자상업거래실현설비의 정의, 개발 및 검사에 어떻게 참가하는가를 규정한다.

개발과제관리자는 그 개발과제의 분담구조를 규정하고 그 개발과제의 진척정도를 측정하는 리정표를 설정한다. 개발과제관리자는 책임분담을 하며 비용예산과 자원예산을 관리한다.

효률적인 개발과제관리가 없으면 전자상업거래계획은 기업의 요구를 만족시키지 못하는 값비싸면서도 결과가 없는 시도로 될수 있다.

개발과제를 계획하고 그것을 철저히 실행하는 능력이 있어야 정확한 원가통제와 계획화결정이 가능하다.

고려할 사항은 다음과 같다.

- 개발과제계획이 측정할수 있는 형태로 최종목표를 정확히 규정하는가.
- 개발과제를 제때에 그리고 계획외의 자원지출이 없이 실행할수 있는 충분한 인적자원과 기타 자원들이 준비되여 있는가.
- 표준적인 개발과제관리검토가 진행되였는가.
- 개발과제지출이 어떻게 장악되는가.
- 실행 및 재정적인 측면에서 개발과제가 자기 궤도에 있는가.

믿 음 성

전자상업거래의 하부구조는 소비자가 그것을 리용하고 싶을 때마다 리용할수 있어야 하며(리용성) 소비자가 바라는대로 동작하여야 한다(무결성). 대부분의 사람들이 인식하고 있지는 못하지만 신뢰성은 보안과 관련되는 기본요소이다. 소비자들은 상품을 전자상업거래를 통하여 살 때 자기들이 거래하려는 상인의 상품명세를 펼쳐 보고 주문상품을 입력하며 임의의 거래도 철저히 마무리되기를 바란다. 그리고 판매자가 자기들의 주문상품이 해당 시간에 도착하도록 체계구성부분들을 다 동작시키고 있을것이라는 확신을 가지고 싶어 한다.

그런데 일이 잘못되면 어떤 일이 생기겠는가. 소비자들은 상인에게 충고를 하고 그 해결책을 찾을수 있도록 판매자와 접촉하는 방법을 요구한다. 그러나 신뢰성은 이런 문제가 해결되는것이상으로 포괄범위가 크다. 신뢰성에는 회사나 기관이 현재 혹은 앞으로 문제가 있을수도 있다는것을 아는 능력까지 포함된다. 체계의 성능은 어떻게 평가되는가, 봉사제공자들중의 한 사람에게 책임이 있는 문제는 어떻게 해결하는가.

성능

체계가 신뢰성 있고 친절하며 가치 있는 경험자료를 제공하는 능력은 본질적이다. 사용자들은 봉사내용, 봉사에로의 접근 그리고 자기들이 요구하는것을 빨리 찾는것 등에 대하여 큰 기대를 가지고 있다. 사용자의 관점에서 성능은 정보가 화면에 현시되는데 걸리는 시간으로 측정된다. 동화상과 보기 좋은 그라픽스가 많은 회려한 Web싸이트는 일단 완전히 내리적재되면 눈길을 끌수도 있지만 그 판매자의 화려한 홈페지가 내리적재시간이 무한정 걸리면 대부분의 사용자들은 실망하며 다시는 보려고 하지 않는다. 최소능력을 가진 체계에 맞추어 개발하면 다른 모든 체계들도 그 페지에 다 접근할수 있을것이다.

성능에 대한 소비자의 견해는 상인의 인터네트접근의 능력계획화와 소비자들에게 봉사를 제공하는 봉사기들에 따라 달라 질수 있다. 상인측이 소비자들이 바라는 실제 성능준위를 보장하지 못하면 결국에는 그 상인자신이 피해를 당한다. 망과 봉사기성능에 관한 능력계획화는 얼마나 많은 사용자들이 그 싸이트에 접근하게 하겠는가에 따라 강화될수 있다.

리유가 어떻든 성능문제를 빨리 해결할수 있는 계획을 작성하는것은 소비자수요를 사전에 예견하는데서 매우 중요하다. 이렇게 되면 팀에 대한 능력계획화전문지식을 가지는것으로 된다. 전문가들은 매일매일 성능을 감시하여 싸이트를 리용할수 있는 소비자들의 수를 최대화하고 래일에는 증가된 사용자들을 처리할수 있는 충분한 능력이 있도록 한다.

구성구조

신뢰성고찰에서 두번째 요소는 총체적으로 체계 및 망구성구조와 관계된다. 소비자들에게 봉사할 때 어떤 체계들이 개입하며 그 체계들이 봉사제공에서 어떻게 호상작용하는가를 리해하는것이 중요하다. 능력계획작성자들이 중요한것처럼 시장에 파악 있는 전자상업거래설계가가 매우 중요하다. 회사전반을 보호하는 보안구조와 그 실현방법을 알고 있는 보안전문가들도 역시 중요하다.

성능측정

능력계획화와 소비자만족 그리고 사용법과 관련한 계측값수집도 필수적이다. 운영통계자료수집은 기업운영의 부분으로 되며 기술사용중단시간과 용도와 같은 항목들을 포함한다. 운영통계자료들은 일반적으로 제기되는 문제에 관한 정보를 제공하는데 리용되며 정확한 운영문제들에 노력을 집중해야 할곳을 판단하는데 도움이 된다. 문의소(help desk) 봉사나 소비자봉사분야는 이 종류의 계측값을 기록하는데는 무의미하다.

운영통계자료가 다 수집되면 분석되고 운영상태보고서를 작성할수 있도록 계측값으로 정리되여야 한다. 전자상업거래환경이 어떻게 동작하고 있는가, 얼마나 많은 소비자들이 싸이트를 리용하였는가, 지출은 얼마이며 무엇이 판매되였는가. 그러나 계측값들은 기관전반에 걸쳐 종합되여 기관이 어떻게 일을 처리하고 있으며 소비자들이 무엇에 관심이 있는가를 최고경영진으로 하여금 판단하도록 전략적지표들을 설정할수 있게 한다. 그 관계를 그림 37－3에 보여 주었다.

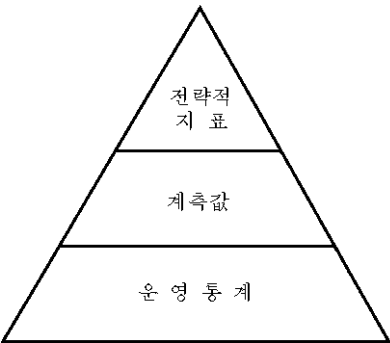



그림 37－3. 운영통계자료로부터 전략지표에로의 이행과정

운영통계자료와 계측값들에 대하여 고려해야 할 사항들에는 다음과 같은것들이 포함된다.

- 리용할수 있는 계측값을 수집, 보고, 확증하기 위하여 어떤 노력을 하고 있는가.
- 내부 및 외부봉사제공자들로부터 어떤 계측값을 받을수 있는가.
- 그 계측값들에 대한 보고서구조결정
- 그 계측값들의 리용방법결정
- 체계를 개선하거나 문제점들을 시정하기 위하여 어떤 공정에서 그 계측값들을 되돌려 리용하는가.

문제해결

전자상업거래싸이트의 기본사용자는 소비자들이다. 그러나 때로는 일이 잘못되거나 소비자들이 그 싸이트를 리용하는 과정에 문제가 생길수 있으며 그 문제에 관하여 누구와 상담하고 싶은 경우가 있다. 결국 소비자들은 그 문제들을 통지하거나 그 대답을 요구할수 있는 장소를 필요로 한다.

이것은 그 Web싸이트에 관한 문제보고서가 작성되고 그 해결을 위하여 정확한 지원그룹에 제출되는 쎈터 혹은 제품에 대한 질문을 하면 그에 대한 대답이 제공되는 소비자문의쎈터의 설립을 요구한다. 그 쎈터를 효률적으로 운영하자면 소비자의 문제와 그에 대한 해결책을 제공하기 위하여 무엇이 진행되였는가 하는 리력을 추적할수 있는 문의추적체계를 리용하여야 한다.

만일 세계적인 회사를 운영한다면 (만일 회사가 전자상업거래싸이트를 가지고 있다면 소비자들은 세계적인 소비자로 될것이다) 사람들이 세계의 임의의곳에서 실시간적으로 회사에 접근할수 있는 방법을 찾아야 할 필요가 있다.

소비자문의쎈터는 소비자의 요구에 빨리 응하여 그들이 긴급하게 요구하는 정보를 제공할수 있어야 한다. 그래야 소비자들이 그 능력에 대하여 확신을 가지며 자기들의 구매경험을 보충할수 있다.

문의쎈터를 고찰할 때 다음의 질문들이 고려되여야 한다.

- 소비자와 회사가 만족준위를 어떻게 평가하는가.
- 일단 통지를 받으면 문제를 해결하는데 얼마만한 시간이 걸리는가, 소비자가 그 해결책에 대하여 만족하는가, 후속대책이 필요한가.
- 통지해 온 문제에서 공통적인 문제가 무엇이며 그것들을 수정하기 위하여 무엇이 진행되였는가.
- 어떠한 문제추적 및 해결체계가 리용되고 있는가.
- 계측값들을 얻을수 있고 추세를 파악할수 있게 문제들이 기록되였는가.

봉사준위협약

봉사준위협약(SLA)은 운영예상성능과 문제확대 및 해결을 포함한 봉사조건들을 규정한다. 전자상업거래활동에서는 운영예상성능과 문제확대 및 해결이 중요하다. 성능이 좋지 않다는것은 전자상업거래봉사를 소비자가 리용할수 없다는것을 의미하므로 제공된 봉사의 운영성능은 관건적인 요소로 된다. 이것은 다시 인터네트상에서의 회사의 최저신용기준선영상에 부정적인 영향을 미칠수 있다.

문제의 시기적절한 해결도 역시 같은 리유로 하여 중요하다. 소비자들은 제기된 문제의 봉사준위시간성이 만족되기를 기대한다. 봉사제공자들과는 어떤 협약이 있으며 그 계약을 지키지 않을 때 처벌이 있는가.

SLA는 봉사제공자들의 능력을 평가하는데 도움이 되며 그 계약을 갱신할 때도 쓸모가 있다. 성능 및 문제해결에 관한 좋은 정보를 수집하고 보관한다면 계약의 변화 그리고 봉사송달에서 좋거나 혹은 좋지 않은 성능에 기인되는 가격을 협상하는데서 더 성공할수 있을것이다.

전자상업거래환경을 위해 준비되여 있는 SLA를 검토할 때 잊지 말하야 할 사항에는 다음의것들이 포함된다.

- ISP와 망제공자들과 같은 제공자들로부터 SLA를 구입해야 한다.
- SLA에는 어떤 봉사의 질조항들이 있는가, 봉사제공자들이 그 협약을 준수하고 있는가.
- 봉사제공자들과 기관이 그들의 사업능률에 대한 기록을 가지고 있는가.

기업유지

체계고장, 접속손실 혹은 기타 문제로부터 회복하는 하부구조의 능력은 본질적인것이다. 상품판매를 위한 주문도 유지되여야 할 매우 중요한 활동이다. 기관이 자기의 전자상업거래의 하부구조의 부분적인 혹은 완전한 손실을 어떻게 처리하는가, 전자상업거래기업을 유지하기 위한 해당한 계획이 준비되여 있는가.

기업지속성계획과 재해복구계획은 그 어느 기업에서나 중요한 문제로 되지만 치명적인 체계고장후에 기업운영을 유지하는데서도 중요하다. 례를 들면 여러 체계들이 갑자기 고장날 때 전자상업거래운영이 유지될수 있는가.

이것은 후원기관에 물어 보아야 할 중요한 질문이다. 만일 기관이 전자상업거래환경의 앞으로의 운영에 크게 의존한다면 짧은 시간동안의 고장도 기업에 재난적인 영향을 미칠수 있다. 만일 기업운영이 최저통화량(foot traffic)에 보다 더 의거하고 있다면 기업운영정지시간(down time)의 여유가 있을수 있다.

그러나 오늘날의 정보시대에 직결기업(online business)이 비직결기업으로 된다면 모두가 그 소문을 매우 빨리 알게 될것이다.

기업지속성에 관하여 관심을 두어야 할 사항들은 다음과 같다.

- 전자상업거래가 기관의 생존에 얼마나 중요한가를 결정하기 위한 업무영향분석이 진행되였는가.
- Web봉사기와 기타 체계들이 비상사태계획의 전자상업거래송달부분에 포함되여 있는가.
- 예비복사절차, 신뢰성 있는 예비본들 그리고 정규적인 자료 및 체계회복검사가 있는가.
- 체계상태감시자가 무결성과 운영을 유지하게끔 되여 있는가.

개 발

이미 앞에서 언급한것처럼 소비자들은 전자상업거래체계가 자기들을 위하여 어떻게 동작하는가에 대한 경험을 기억하고 있을것이다. 그러므로 일관성 있는 대면부를 개발하는것이 필요하며 그것은 충분한 개발실천을 통하여 달성될수 있다.

표준과 관례

소비자들이 전자상업거래싸이트리용에서 긍정적인 경험을 가지도록 하는 기본방법은 개발표준과 관례를 수립하는것이다. 이것은 소비자들의 거래경험에서 쌓은 감각과는 다르다.

싸이트개발자들은 응용프로그람들이 어떻게 개발되는가에 대한 정보와 방법을 제공하기 위하여 표준과 관례를 리용한다. 여기에는 코드표준과 보안 그리고 소비자로부터 제출된 정보가 어떻게 확인되고 보호되는가 하는것과 같은 문제들이 포함된다. 따라서 보안은 후에 생각나서 응용프로그람에 포함되는것이 아니라 처음부터 응용프로그람에서 고려될 필요가 있다.

개발자들은 자기들의 경험과 교육에 기초하여 체계의 구체적인 부분을 어떻게 개발하고 작성할것인가에 대한 결심을 채택한다. 여기서 잘못하면 계속적인 유지와 뒤따르는 고장퇴치 및 문제해결이 어렵게 된다.

변경조종과 변경관리

변경조종(change control)은 전체 개발/생산주기에서 관건적인 부분이다. 적절한 변경조종은 생산에 도입된 불철저하게 검사된 응용프로그람의 위험을 감소시킨다. 변경조종은 또한 매일매일의 변경으로부터 응용프로그람코드에서의 변경까지 식별하는데도 쓰이며 적절한 문제해결과 개발자교육을 가능하게 한다.

응용프로그람코드의 개발과 관련한 기본문제는 그것이 흔히 생산체계에 삽입되며 소비자들이 그것을 리용하는 동안에 《수정》된다는 사실이다. 이 형태의 활동은 체계의 개발에 영향을 줄뿐아니라 전자상업거래싸이트에 대한 사용자의 인식과 기업의 직결존재

에도 영향을 준다.

정확한 변경조종은 개발코드가 개발환경에서 검사되고 소비자가 제공하는 정확한 정보만이 아니라 고의적인 혹은 우연적인 입력에서의 처리오차를 처리하게끔 한다.

Web싸이트에 수집된 정보의 정확한 처리는 기업운영에 영향을 미친다. 정보를 정확히 처리하지 못하면 소비자에게 적당치 않은 책임을 전가할수도 있다. 다시 말하면 송달오유는 상품을 잃게 하거나 지출을 증가시킨다.

구성과 변경조종환경을 평가할 때에는 다음의 사항을 고려하여야 한다.

- 응용프로그람코드변경과 조작체계변경을 다 포함하는 쏘프트웨어출하판변경통제 및 판본통제
- 빨리 발전하는 오늘의 세계에서 안전한 조작환경을 유지할수 있는가, 변경처리를 자동화할수 있는가.
- 개발, 실현 및 이전(migration)표준

접 속 성

접속성은 구체적으로 공공망과 개별망에로의 망접속성, 리용가능한 대역너비를 어떻게 계산하며 망이 어떻게 설계되는가를 정립하는데 리용되는 기술과 관련된다. 전자상업거래는 소비자들이 Web싸이트를 특히 겨울휴가때 리용할수 있도록 망설계를 잘했는가와 충분한 수용능력이 있는가에 의존한다.

이것은 충분한 인터네트접속속도와 수용능력을 의미하며 또한 전자상업거래설계에서는 그만한 접속속도와 수용능력을 가진 회사망에로의 접속을 의미한다. 많은 망설계가들은 자기 분야에서는 주도자이지만 충분한 망수용능력에 대해서는 쉽게 무시하는 경향이 있다.

망이 지나치게 큰 수용능력과 기타 자원들을 가지고 지나치게 크게 구성되면 필요없이 회사자원을 랑비하게 된다. 기업들은 시장거래와 판매계획을 세우고 예상되는 통화량을 처리하며 수요가 증가할 때마다 규모를 적절하게 조절할수 있는 유능한 기술경영자와 망설계가들을 가지고 있어야 한다.

망설계가들은 전자상업거래싸이트를 적당한 위치에 배치하여야 한다는것을 리해하여야 한다. 이것은 만일 망을 세계적규모로 운영하려고 할 때 소비자들에게 최량의 신속성과 성능을 담보하도록 여러 위치에 배치하는것을 고려하여야 한다는것을 의미한다. 이것은 공정에서 환경의 복잡성을 증대시킬수 있고 나아가서 철저한 계획화에 대한 의존성을 증대시킨다.

그 계획화부분에는 여유계획화도 포함되는데 그것은 비상사태와 기업지속계획화의 부분으로 된다. 만일 어떤 리유로 하여 하나의 요소나 위치를 리용할수 없게 된다고 하여도 존재를 유지할수 있고 전자상업거래기업의 운영을 계속할수 있다.

소비자들은 전자상업거래환경과 거래할 때 긍정적이면서도 고무적인 경험을 얻고 싶어 한다. 이런 경험을 제공하지 못하면 회사싸이트의 직결존재에 부정적인 후과가 초래

된다. 이것은 회사가 전자상업거래를 처리할수 있게 준비되여 있지 않다는 인식을 줄수 있으며 소비자들은 마지 못해 싸이트와 거래를 진행하게 된다.

망접속성과 관련하여 다음의 사항들을 잊지 말고 고려하여야 한다.

- 전자상업거래싸이트의 위치
- 망수용능력
- 망리용가능성의 유지 및 감시
- 망위상구조
- 망의 여유
- 보안
- 송신련결점들이 얼마나 안전한가
- 절환된 망을 리용할수 있는가
- 전자상업거래송달에서 어떤 형식의 가상개별망(VPN)이 리용되는가

보 안

보안분야를 구성하는 네가지의 주요한 요소들은 다음과 같다.

1. 접속의 의뢰기측 혹은 사용자측
2. 망전송체계
3. 전송하는 동안의 망정보보호
4. 사용자식별과 인증

전자상업거래의 하부구조에 상주하고 있는 망보안요소 및 콤퓨터체계를 보호하는것은 자료의 무결성을 보호하며 법률적인 그리고 최량의 실천적인 요구를 만족시키는 주요부분이다. 이 보호준위는 각이한 수단을 통하여 실현되는데 그 수단들은 협동적으로 동작하여 방위심도를 보장해야 한다.

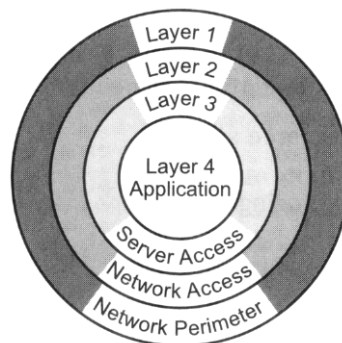



그림 37－4. 보호준위

그림 37－4에서 보는것처럼 계층화는 보호준위가 중심방향으로 증가하는 동심원들의 렬로 직관화할수 있다. 층 1 혹은 망주위는 망자체에로의 허용되지 않은 접근을 차단한다. 이것은 방화벽과 원격접근봉사기 등을 포함한다. 층 2는 망이다. 일부 정보는 아무러한 고려도 없이 망에서 처리된다. 층 2는 자료가 망안에서 이동할 때 자료를 보호한다. 이 기술에는 련결암호화프로그람, VPN 그리고 IPSec가 포함된다.

층 3은 봉사기체계자체에로의 접근을 고려한것이다. 많은 사용자들은 봉사기에로 접근할 필요는 없지만 봉사기에 상주하는 응용프로그람에 접근한다. 그러나 봉사기에 접근한 사용자는 자기에게 필요한것보다 더 많은 정보에 접근할수 있다. 그러므로 층 3은 봉사기자체에 대한 접근 및 조종을 진행한다.

마지막으로 층 4는 응용프로그람준위의 보안을 진행한다. 매개 응용프로그람이 보안을 어떻게 처리하는가 혹은 어떻게 처리하지 못하는가 하는 문제에서의 불일치로 하여 많은 보안문제들이 존재한다. 여기에는 그 응용프로그람내의 구체적인 기능들에 대한 접근과 허용이 포함된다.

기관들이 좋은 기술을 잘못된 방식으로 실현하는 경우가 있을수 있다. 례를 들어 사용자가 잘못 구성한 최고의 방화벽은 싸이트에로의 불필요한 통화량을 저지시키지 못하며 또는《공개》접근으로 인정된 모든 자료표들을 가지고 있는 자료기지보안체계는 자료들을 보호하지 못한다. 이것은 일반적으로 보안에 대한 그릇된 인식을 초래할수 있으며 기관을 자기 만족감에 사로잡히게 할수 있다.

그러므로 매개 층을 련결하여야(그림 37－5를 볼것) 사용자가 일부 경우에 보지 못하는 보안을 제공할수 있으며 최소한의 거래로 필요한 봉사에로의 접근을 보장할수 있다. 매개 층사이의 통합은 이것을 가능하게 한다.

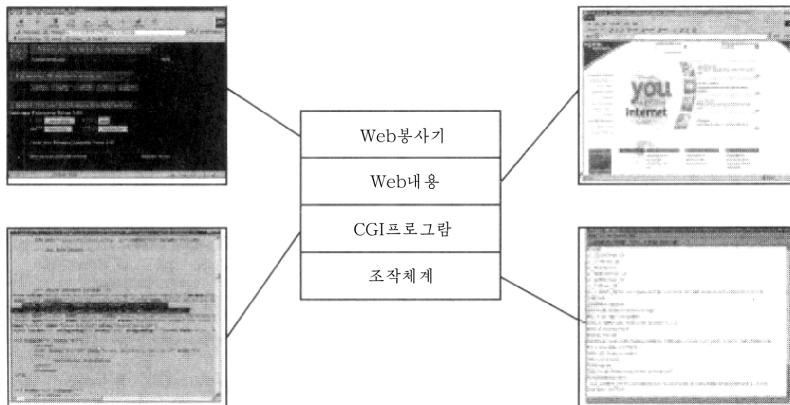



그림 37－5. 층련결

전자상업거래환경내에서 보안을 실현하는 경우에도 사정은 마찬가지이다. 보안은 매개 층 즉 의뢰기, 망, 망주변 그리고 련관된 봉사기들에서 고려되여야 한다. Web대면부는 4개의 기본층 즉 조작체계, CGI프로그람들, Web내용 그리고 Web봉사기를 가지고 있다. 매개 층은 정확하게 동작하는 다른 층들의 요소에 의존한다.

의뢰기측(사용자)

의뢰기는 자기의 Web열람기를 통하여 전자상업거래의 하부구조와 호상작용한다. 그러나 사용자들은 그 호상작용이 어떻게 보이고 작용하며 그리고 자기들의 콤퓨터에서 어떻게 실행되는가에 대하여 일정한 기대를 가지고 있다. 경험이 긍정적인것으로 되자면 설계, 개발 및 실현단계에서 일정한 프로그람작성을 고려하여야 한다.

사용자들이 가지고 있는 경험은 열람기실현방식에 따라 서로 다를수 있으며 다른 열람기에 의하여 지원되지 않는 열람기확장지원을 선정하는것은 좋은 기업결정이 아니다. 동적인 HTML과 그라프적내용들은 리용되는 각이한 Web열람기와 량립되여야 한다. 전자상업거래응용프로그람은 이 요구조건을 고려하여야 한다. 모든 사용자들이 Cookie, Java, Java Script와 같은 열람기에서의 확장된 특성들을 허용하려고 하지는 않는다. 이것은 응용프로그람설계에서 제공될수 있는 기능에 영향을 준다.

봉사를 리용하는 사용자와 기업들이 인터네트에 직접 접속되지 않을수도 있다. 그들은 대리자봉사기를 리용하여 보안을 제공하거나 또는 망요청을 완충시킬수도 있다. 또한 저속의 망련결을 리용할수도 있다. 이 인자들도 긍정적인 경험을 유지하기 위하여 설계에 포함되여야 한다.

의뢰기측문제를 고찰할 때에는 다음의 사항에 주의를 돌려야 한다.

- 어떤 형태의 Web열람기와 대리자봉사기가 리용되고 있으며 동작환경이 어떤가를 조사하는것
- 소비자가 전자상업거래접근을 어떻게 등록하는가를 판단하는것
- 전자상업거래대면부리용의 용이성을 판단하는것
- 대면부개발에 어떤 응용프로그람이 리용되는가를 확인하는것

방화벽

방화벽은 전자기업구조의 필수불가결의 부분이다. 보호가 없이 인터네트에 직접 접속된 임의의 콤퓨터는 회생호스트로 인정된다. 어떤 점에서 그 콤퓨터는 취약성을 가지게 될것이다. 방화벽리면에 모든것을 숨겨 놓는것은 불합리하며 인터네트에 직접 보여줄 필요가 없는 매개 체계는 방화벽에 의하여 보호되여야 한다. 그리고 보호되지 않은 임의의 체계는 방화벽을 통과하여 회사망에 직접 접속되지 말아야 한다.

그러나 비무장지대(DMZ)와 봉사망들을 리용함으로써 망설계에서 방화벽은 강화될수 있다(그림 37－6). DMZ는 경로기안에 있는 려파기와 접근조종목록을 통하여 체계를 보호한다. 봉사망은 방화벽에 련결된 개별적인 망이다. 직접적인 인터네트접속을 요구하지 않으며 회사망에 있을 필요가 없는 임의의 체계는 봉사망에 놓인다.

소비자는 DMZ에 있는 체계와 호상작용한다. 소비자에게 경험을 제공하는데 필요한 추가적인 봉사는 봉사망에 들어 있는 체계에 의하여 보장된다. 회사망의 체계로부터 회복되여야 할 임의의 보충적인 정보는 중간봉사기들에 의하여 회복된다. 이것은 지나치게 복잡한 배렬구조인것 같지만 설계상 보안정도가 아주 높다. 방화벽밖의 체계들은 회사

망에 접속할 능력이 없다. 방화벽은 DMZ로부터 봉사망에로의 접속 그리고 구체적인 IP 주소들 및 망봉사에로의 접속망을 허용하도록 되여 있다. 그러면 봉사망의 내부체계는 필요한 정보를 얻기 위하여 회사망내부의 체계와 접속할수 있는 권한을 가진다.

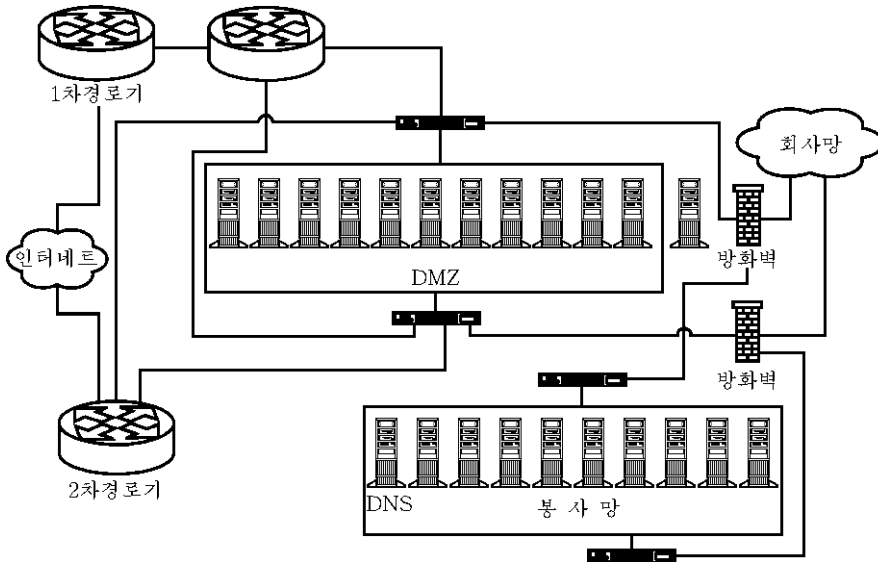



그림 37－6. 비무장지대(DMZ)와 봉사망들

침입탐지체계들의 리용 그리고 취약성평가도구에 의한 주기적인 평가는 또한 봉사의 성격과 공격의 가능성때문에 전자상업거래보안구조의 한 부분으로서 반드시 강조되여야 한다.

방화벽과 망보안실현을 고찰할 때 다음의 사항을 검토해야 한다.

- Cybercop 혹은 ISS와 같은 망취약성도구를 리용하고 있는 모든 망요소들의 취약성실태보고서
- 잠재적인 공격점들을 감소시키도록 체계들이 《경화》되여 있는가를 판별하기 위한 DMZ체계들
- Web의뢰기와 봉사기가 어떻게 SSL암호화와 교섭하며 어떤 암호화장점이 제공되여 있는가.
- 보안내부관계를 조사하고 분석하기 위하여 방화벽을 통하여 열려 진 비HTTP포구들
- 방화벽위상구조
- 방화벽구성파일
- 망장치들의 접근조종목록
- 망통신규약
- 망보안요소들에 대한 구성관리

전자상업거래봉사기의 보안

전자상업거래봉사기는 기업봉사를 제공하기 위하여 접속된 다양한 모든 요소들로 구성되여 있다. 매개 체계를 철저히 보안하는 기회들을 리용할 목적으로 임의의 단일체계의 복잡성을 감소시키는데 여러개의 체계들이 리용된다. 이 봉사에는 HTTP나 Web봉사기자체, 개별화체계들, 등록부체계들, 전자우편관문들 그리고 인증체계들이 포함된다.

디렉터리봉사

디렉터리봉사는 등록된 사용자들과 그들의 련관정보를 담은 직결보관소를 유지하는 기능을 제공한다. 그 정보에 대한 중심보관소를 리용함으로써 사용자에 관한 인증자료나 정보를 요구하는 임의의 체계들이 그것에 접근할수 있다. 그리고 응용프로그람들은 인쇄정보를 주문하거나 요청할 때 혹은 생산품을 사용자들에게 운반할 때 사용자들의 우편정보를 비롯한 사용자에 관한 정보를 요구할수 있다.

여러개의 디렉터리체계들을 리용할수 있지만 X.500과 경량디렉터리접근규약(LDAP)에 기초한 체계들이 가장 높은 준위의 통합과 리용성을 제공한다.

사용자에 관한 모든 정보들은 중앙보관소에 보관되여 있기때문에 그 체계들에 있는 정보를 보호하며 그 자료에 대한 인증되고 안전한 전송통로를 제공하는데 특별한 주의를 돌려야 한다. 보관소는 리용성이 높아야 하며 많은 체계들은 요청을 받을 때 정보를 제공할수 있는 보관소의 능력에 의존할것이다. 앞에서 언급한것처럼 자료의 통합정리는 정보가 보관될 때와 망을 통하여 전송되는 사이에 경영관리자들이 더 쉽게 신뢰성을 보장하고 무결성을 유지할수 있게 한다. 한편 자료를 통합정리하면 체계가 공격목표로 되지 않겠는지 하는 위구심을 가질수 있다. 그러나 집중화는 망보안전문가들에게 체계를 보호할수 있는 기회를 보장한다.

제공된 디렉터리봉사를 평가할 때 고려할 점은 다음과 같다.

- 얼마나 많은 자료가 보관되는가.
- 얼마나 빠른 디렉터리응답을 보장하여야 하는가.
- 단번에 얼마나 많은 디렉터리질문을 처리할수 있는가.
- 디렉터리에 어떤 보안기능이 통합되는가.
- 디렉터리가 인증된 접속을 지원하는가.
- 소비자가 그 자료가 보관되는 중이라는것을 아는가.

우편봉사기

전자우편은 임의의 전자상업거래하부구조에서 기본구성요소로 된다. 전자우편은 전자상업거래하부구조체계로부터 사용자나 기업에 정보를 송달한다. 소비자들은 전자우편에 의거하여 정보를 요청하며 질문이나 문제가 제기될 때에는 소비자봉사 혹은 후원자들

과 상담한다. 전자우편은 또한 소비자들이 경험에 대하여 좋다 아니면 좋지 않다는것을 통지하는데도 리용될수 있다. 전자우편은 많은 용도에 리용되지만 특별한 보안을 요구하는 정보의 전송통로로는 리용되지 말아야 한다. 전자우편을 통하여 전송된 정보는 우편만큼 공개적이다. 따라서 신용카드와 구입정보는 물론 사용자이름과 암호는 전자우편을 통해서는 류통되지 말아야 한다. 이것은 S/MIME와 같은 암호화기술에 의해서만 가능하며 안전하게 될수 있다.

우편봉사기의 운영은 하부구조운영에서 관건적이다. 전자우편봉사기들은 또한 해커들이 다른 체계들에 접근하거나(흔히 기본보안위험으로 간주되지 않는) 대용량의 비요청 전자우편물들을 산포하기 위하여 흔히 리용한다. 현재 리용할수 있는 상업적우편봉사기들가운데서 많은것들은 정보를 보호하고 공개할수 있는 그 구조와 관계되는 특징을 가진다. 외부사용자가 자기가 회사직원인듯이 전자우편을 발신하거나 혹은 다른 우편봉사기들에 전자우편문서를 중계하는 우편봉사기를 리용하여 전자우편을 발신하도록 잘못 설정된 우편봉사기도 있다는것을 생각해야 한다.

이런 실례들은 보안업계에서 매일과 같이 보고서로 작성발표되는데 그것은 일반적으로 간단한 설정상오유와 낡은 쏘프트웨어의 리용 혹은 쏘프트웨어보강수정판본으로 갱신하지 않는것과 관계된다.

전자우편의 보안과 리용성을 고찰할 때 고려할 점은 다음과 같다.

- 어느 우편송달대리자(MTA)와 우편사용자대리자가 리용되고 있는가.
- 우편송달대리자의 설정파일에 대한 접근허가
- 비법리용가능성을 판단하기 위한 우편봉사기의 송달 및 오유
- 운영기록의 주기적인 조사
- 다양한 공격에 대한 취약성을 검사하기 위하여 MTA의 일반적인 《해커용약점》을 조사하는것
- 비루스방지기술의 리용평가
- 내용관리와 암호화기술

Web봉사기

Web봉사기는 전자상업거래하부구조에서 가장 관건적인 요소로 간주되고 있다. 사용자에게 Web에서 볼수 있는 내용들을 송달하고 사용자나 다른 체계들에 정보를 회복시키거나 보내는 프로그람을 실행하며 요청의 유효성을 판단하기 위한 특수한 검사를 진행할것이 요구된다. Web봉사기는 언제나 리용할수 있고 허용시간내에 사용자의 요청에 응답할수 있어야 한다. 만일 망이 불완전하거나 Web봉사기의 성능이 좋지 못한 탓에 사용자들이 기다려야 한다면 그들은 즉시 그 싸이트를 포기할것이다. 사용자들도 또한 그 기업에 대하여 부정적인 인식을 가지게 될것이고 다시는 그 싸이트를 리용하려고 하지 않을것이다.

많은 Web봉사기들은 상업적쏘프트웨어, 무료쏘프트웨어들을 리용할수 있다. 가능하다면 문제가 제기되여 쏘프트웨어에 대한 판매회사의 보수작업이 필요한 때에는 상업적인 실현형태를 구입하여 신속히 지원을 받을수 있다. 무료쏘프트웨어인 경우 초기지출이

작을수 있고 그것들이 매우 견고할수는 있지만 설치후 수리 및 지원원가는 대단히 높을수 있다. 회사가 파산되였거나 자유롭게 사용하는 설비를 관리하는 전문가들이 은퇴한 경우를 고찰하자. 이 경우에는 그 설비에 정통한 사람을 찾기보다 상업적인 쏘프트웨어에 유능한 전문가를 찾는것이 훨씬 더 쉬울것이다.

Web봉사기자체를 구성하는데는 응용프로그람의 설계와 Web내용에 대한 개발규격이 필요하다. Web봉사기쏘프트웨어는 어떤 특수한 허가나 혹은 행정적인 허가가 필요한 체계에서 실행되지 말아야 한다. 그래야 공격자가 봉사기의 신용을 떨어 뜨리기 위하여 행정적인 우선권을 획득할 위험성이 감소된다.

봉사기의 운영은 또한 응용프로그람들과 문서양식들에로의 접근을 보장하는 CGI스크립트들의 리용가능성에도 의존된다. CGI프로그람들은 보안과 관련한 문제를 일으키는 잘못 쓴 코드가 나타나지 않는다는것을 담보하기 위하여 개발할 때와 최종적으로 공개하기전에 세밀히 조사되여야 한다. 비밀성과 무결성에 대하여서는 여러번 언급되였다. Web봉사기는 안전소케트층(SSL)이나 전송층보안(TLS)을 통하여 암호화된 론리적련결을 제공할수 있어야 한다. SSL과 TLS는 다 추가적인 하드웨어를 요구하지 않으며 다 봉사기측 인증서를 리용한다. 싸이트에 대한 인증서의 발행은 이 론문의 범위를 벗어 난다. 여러 신뢰회사들이 Web봉사기에 대한 인증서를 발행할수 있다.

SSL이나 TSL에 의하여 기관과 소비자는 현시되거나 전송되는 정보가 망을 통과하는 동안에 보호되고 있다는 확신을 가질수 있다.

Web봉사기와 관련하여 다음의 사항들을 고려하여야 한다.

- Web봉사기가 가동하는 환경에서의 사용자ID허가와 구좌허가를 검토하는것.
- 어느 Web싸이트가 공적인것이고 어느것이 접근이 통제되는것인가를 판별하는것.
- HTML문서들, ASP와 CGI, 디렉터리들과 스크립트들에 대한 접근허가를 분석하는것.
- 마이크로쏘프트IIS 혹은 다른 Web봉사기응용프로그람구성과 운영기록파일들을 조사하는것.
- Web봉사기에 의하여 열람기의 접수된 요청들이 어떻게 확인되는가를 결정하는것.
- 후단처리장치에 전송된 요청들이 어떻게 확인되는가를 결정하는것.
- Java, JavaScript, XML을 포함하여 Web에 기초한 응용프로그람 및 자료기지접속성을 조사하는것.
- 잘 알려 져 있는 ASP와 CGI스크립트 그리고 보안위험이 있는 편의프로그람이 존재하는가를 검사하는것.
- Web 및 대리자봉사기구성파일들을 조사하는것.
- SSL통신을 가능하게 하는 Web봉사기구성파일과 인증서들을 검사하는것.
- 전자상업거래봉사에서 리용가능성이 높은 요소들을 분석하는것.
- 관건적인(중심) 봉사기의 조작체계와 Web쏘프트웨어패치준위 그리고 구성파일들을 평가하는것.
- 응용프로그람패치준위와 구성파일을 평가하는것.
- 외부적인 전자상업거래체계들이 내부체계에 어떻게 인증되는가를 판단하는것.

- 봉사인증서를 발행하고 소비자가 인증서의 확실성을 인정하게 하는 방법이 있을 때 인증권한을 고려하는것.
- 부인방지특성의 요구조건을 평가하는것.
- CGI스크립트를 평가하고 프로그람코드를 검사하는것.
- Web내용관리를 고려하는것.

조작체계보안

이미 설명된 모든 구성요소들은 조작체계가 제공하는 기초봉사에 의거한다. 개별적인 응용프로그람의 매개 요소들은 더 안전하게 될수 있지만 확고하면서도 안전한 기초가 없어도 다른 노력들에 영향을 미친다. 현재 대다수의 전자상업거래체계들은 Windows NT 혹은 UNIX조작체계상에서 가동하고 있다. 매개 환경은 자체의 우단점과 체계의 취약성을 가진다.

Windows NT조작체계

Windows NT는 임의의 하부구조에서 특수한 계산과제들을 수행하는데 리용되는 인기 있는 조작체계이다. 이 조작체계를 정확하게 구성하는것이 중요하다. 만일 그것이 정확하게 구성되지 않고 보안이 정확하게 실현되지 않는다면 쉽게 약화될수 있다.

Windows NT는 조작체계와 응용프로그람구성을 설정하는 체계관련정보를 보관하는 파일에 크게 의존한다. Windows NT에서 여러개의 주요봉사는 같은 망봉사포구로 진행된다. 이것은 원격사용자에게 체계를 조사하고 중요한 체계관련정보를 보관하는 파일정보를 수집하는 능력을 제공한다. 디스크공유정보, 사용자이름 그리고 체계의 구체적인 구성과 같은 정보를 장악하면 체계에 대한 성공적인 공격을 단행할수 있다.

Windows NT를 전자상업거래조작체계가동환경으로 사용할 때에는

- 호스트 및 망에 기초한 취약성스캐너를 리용하여 전자상업거래봉사를 제공하는 모든 Windows NT체계들의 스캔을 진행할것. 그 결과를 분석하고 조작체계에 있는 포구들이 인증되지 않은 접근에 람용되는가를 조사할것.
- 불필요한 봉사 및 포구를 조사할것.
- 중심봉사기의 체계관련정보보관파일, 조작체계패치준위 그리고 구성파일들을 조사할것.
- 조작체계요소들에 대한 구성배치 및 변경관리를 평가할것.
- 비루스방지기술을 실현할것.

UNIX조작체계

UNIX조작체계는 일련의 각이한 과제들을 수행하는데 리용되는 다중사용자, 다중처

리환경을 제공한다. 그러나 Windows NT와 마찬가지로 보안모듈들과 조작체계의 부정확한 구성은 그 신용을 떨구게 된다. UNIX는 Windows NT보다 훨씬 더 일반적인 전자상업거래환경이다. 조작체계가 상대적으로 완성되였음에도 불구하고 UNIX실현과 관련한 새로운 문제들이 주마다 발견된다. 일련의 조작체계보안문제들에 대하여 대중보도매체들에서도 떠드는것은 그만큼 콤퓨터사용체계가 조작체계에 의존하고 있는것과 관련된다.

Windows NT와 마찬가지로 UNIX는 안전한 조작체계지향형은 아니다. 임의의 보안전문가도 조작체계에 있는 보안체계를 무능하게 하는 많은 방도들을 내놓을수 있다. 조작체계를 견고하게 하고 전자상업거래환경에서의 취약성을 감소시키자면 상당한 노력이 필요하다. 다중사용자조작체계로서의 UNIX는 체계기능의 대부분을 제공하는 망에 기초한 많은 봉사기능을 가지고 있다. 그 봉사와 포구들가운데서 많은것은 전자상업거래기능을 제공하는데 필요한것이 아니다. 그 봉사들은 흔히 비밀성, 자료무결성 및 체계리용성에 대한 공격을 개시하는데 리용된다.

UNIX를 전자상업거래조작체계로 리용할 때에는 다음의 사항을 확인하여야 한다.

- 호스트 및 망에 기초한 취약성스캐너를 리용하여 전자상업거래봉사를 제공하는 모든 UNIX체계들을 스캔하며 그 결과를 분석하고 조작체계에서 포구들이 비법접근에 람용되는가를 검토하는것.
- 불필요한 봉사와 포구들을 검토하는것.
- 관건적인 봉사기들에 있는 조작체계보강수정판준위와 구성파일들을 평가하는것.
- 조작체계구성요소들에 대한 구성 및 변화관리를 평가하는것.

BackOffice응용프로그람

전자상업거래하부구조는 상품명세서를 보고 상품을 주문하기 위한 탐색엔진, Oracle, BaaN, SAP를 비롯한 각이한 BackOffice응용파의 통신경로를 가지고 있다. 이 체계들이 충분히 보호되는것은 물론이고 망을 통하여 전송된 자료들도 충분히 보호되는것은 보호된 정보접근을 제한하기 위해서이다. 게다가 그 응용프로그람들과 관련한 특수한 성능 및 보안문제들도 있다.

탐색엔진

탐색엔진은 전자상업거래환경내에서 특별한 문서나 Web페지를 탐색하는데 리용된다. 탐색엔진의 성능은 Web경로와 페지를 얼마나 빨리 횡단하여 관련자료가 있는 위치에 대한 목록을 생성하는가 하는데 의존한다. 대부분의 탐색엔진들은 그 작업을 두 단계로 수행한다. 첫 단계에서 탐색엔진은 Web페지들을 《더듬으면서》 정보를 수집한다. 두번째 단계에서 탐색엔진은 사용자가 탐색을 요청할 때 사용하도록 탐색가능한 색인을 만든다.

각이한 탐색엔진들은 정보수집에서 각이한 수준의 성능을 제공한다. 이것은 사용자

가 탐색을 요청할 때 탐색결과의 유효성에 영향을 미친다. 만일 탐색을 요청하였을 때 존재하는 페지들을 탐색할수 없다면 사용자는 정보가 존재하지 않는다고 생각할것이다. 이것은 사용자에게 그 Web싸이트에 대한 좋지 못한 인식을 줄수 있다. 더는 존재하지 않거나 관계도 없는 정보를 포함하는 페지들이 나타난다면 사용자는 실망하고 말것이다.

례를 들어 그림 37－7의 그라프를 고찰하자. 두 그라프는 정확히 같은 하드웨어상에서 동작하고 두개의 서로 다른 탐색엔진에 대한 기본체계의 활동을 보여 준다. 우에 있는 체계는 더듬는 단계와 색인화단계에서 체계의 자원을 훨씬 잘 리용한다. 체계자원들을 잘 리용한다는것은 엔진이 효과적으로 동작하고 있다는것을 의미한다. 아래그라프는 훨씬 낮은 자원리용을 보여 주며 이것은 같은 하드웨어자원에도 불구하고 표준작업량을 처리할수 없을수도 있다는것을 의미한다.

탐색엔진과 사용자의 호상작용도 매우 중요하다. 만일 탐색엔진자체가 정확히 실행되지 않는다면 쏘프트웨어나 혹은 탐색이 진행되는 하드웨어때문에 탐색을 포함한 동작이 느릴수 있다. 일부 탐색엔진들은 동시적인 탐색을 잘 처리하지 못한다. 실현에 앞서 모의부하검사(simulated load testing)도 해보면서 제품을 주의깊게 검토하는것이 필요하다.

Basic System Activity

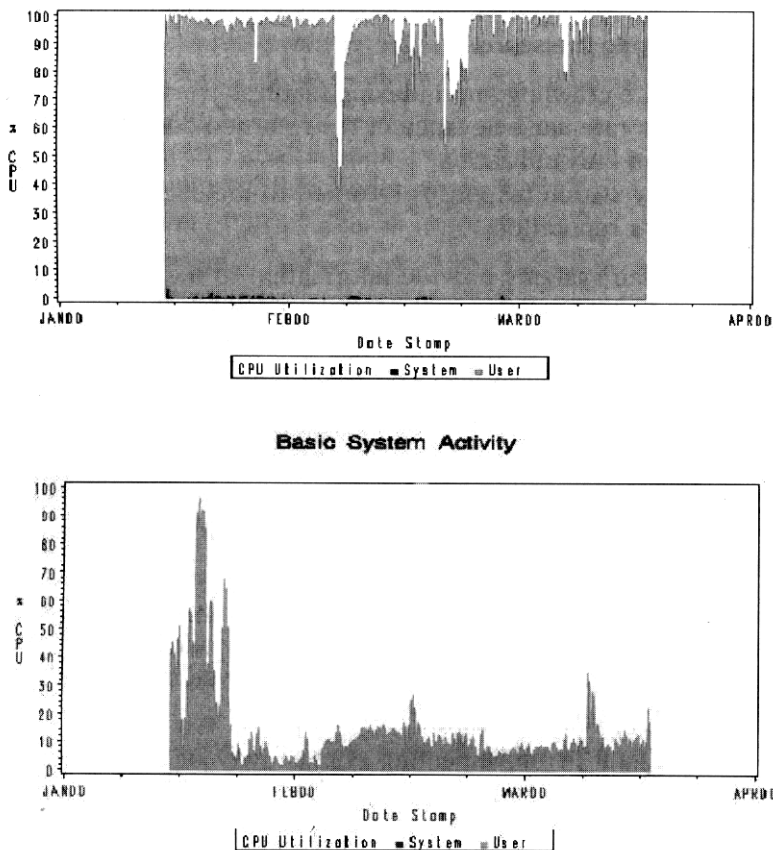



그림 37－7. 두개의 각이한 탐색엔진에 대한 기본체계의 활동

탐색엔진을 평가할 때에는 다음의 사항을 조사하여야 한다.

- 더듬는 기능과 색인화기능이 얼마나 잘 동작하는가.
- 결과본문의 성공률과의 련관성
- CPU와 LAN리용
- 탐색응답이 사용자에게 얼마나 빨리 돌아 오는가.
- 제작업체의 명성

BackOffice체계들은 전자상업거래사용자에게 기관이 엄격한 통제를 유지하려고 하는 정보를 제공한다. 일반적으로 그러한 체계들은 회사의 기타 일상업무를 보장하는데도 리용된다. 이 체계들은 일반적으로 회사망의 보호안에 있으므로 보호된것으로 볼수 있다. 더욱더 많은 사용자들과 소비자들이 봉사 및 접근기술을 요구하기때문에 《철옹성 같은 망울타리》라는 개념은 현실성이 더욱더 적어 지고 있다. 그러나 개발, 응용, 조작체계구성에 관하여 앞에서 제시된 모든 문제들도 여기에 적용되여야 한다.

외부전자상업거래체계로부터 이 체계들에로의 통신은 방화벽에 의하여 조종된다. 방화벽은 해당한 외부체계들만이 해당한 내부체계와 통신하게 하며 따라서 공격이 있는 경우 총체적인 파괴, 약화위험을 최소화한다.

접속의 실현과 이 BackOffice체계의 보호에서 성과여부는 자료가 한 체계로부터 다른 체계로 어떻게 이동되는가, 어떤 규약과 전송방법들이 리용되는가, 누가 자료를 구축하는가, 누가 수신콤퓨터에서 그 자료를 처리하는가 그리고 정보 그자체의 기밀성에 대한 철저한 리해에 의존한다.

BackOffice체계에로의 접속을 평가하고 실현할 때에는 다음의 사항들을 평가하여야 한다.

- 기관의 기밀자료의 보호에 대한 평가
- BackOffice 요소들에 대한 구성관리평가
- 비루스방지기술의 리용에 대한 평가
- 자료기지구성과 관리실천에 대한 평가
- Web싸이트로부터 주문관리체계에로의 주문송달평가
- 주문실현과정평가

결 론

이 론문에서는 전자상업거래구조의 구성요소들을 고찰하고 기관이 그 환경을 개발하거나 검열준비를 할 때 무엇에 중심을 두어야 하는가를 고찰하였다. 이 론문은 결코 매개 기술령역에 대한 완벽한 검토는 아니지만 전자상업거래환경을 구성하는 다양한 요소들사이의 관계와 의존성을 보여 주는데 목적이 있다.

전자상업거래환경의 실현은 임의의 회사로 하여금 경제적으로 세계적인 위치를 차지하며 세계시장에 성공적으로 진출할수 있게 한다. 사실상 일부 소매상인들은 전자상업거래의 덕택으로 벽돌과 세멘트로 지은 실지 상점건물도 거의 가지고 있지 않는다.

모든 측면에서 남들의 눈에 띄우게 하며 기억에 남게 하는것이 아주 중요하다. 빨리하고 서두르고 정확하게 하라. 그렇지 않으면 파산되고 만다.

이것이 전자상업거래의 본성이다. 만일 처음에 정확하게 해놓지 않으면 후에는 그것을 수정할 시간이 없을것이다. 이것은 전자상업거래의 미궁이다.

제 8 편
업무지속성계획화와 재해복구계획화

정보체계와 정보처리의 지속성은 많은 자연적 및 인공적위협을 받고 있다. 기관들은 잠재적인 업무파산에 대하여 항시적으로 대처하고 있어야 하며 자기들의 자동화체계에 대한 회복계획을 검사해야 한다. 더우기 이런 기관들은 지속성계획화공정을 계속 재구성해야 하며 이때 분산형콤퓨터사용환경과 월드 와이드Web 등의 발전하는 기술들의 도전에 부닥친다.

업무지속성과 재해복구를 담보하기 위한 노력은 이미 IT환경에서 하나의 도전으로 되였다. 우리는 현재의 콤퓨터사용환경이 몇년전에 비하여 관리하기가 더 복잡해 졌다는 것을 확신할수 있다. 체계들이 보다 더 분산됨에 따라 그 체계의 조종과 관리가능성이 중심원천으로부터 더욱 더 멀어지고 있다. Web응용세계에서는 많은 조종권이 자원을 소유하고 있는 기관의 밖에 놓인다. 그리하여 관리과정에서 경영진이 지속성계획화(CP)가 중요하다는것을 잘 아는것은 응당하다. 그러나 그 계획을 효과적으로 실행하지 않고 있다.

이 편에서 독자들은 각 기관들이 우발적인 사고에 체계적인 방법으로 대처하고 그 가치를 평가하기 위한 조치를 강구해야 한다는것을 알게 된다. 업무지속성계획화의 필요성은 기관이 계속 생활력을 유지하도록 하는 중대한 체계과제들이 제때에 예비싸이트에서 처리됨으로써 업무에 심각한 영향을 주지 않도록 하자는데 있다. 이런 중대한 처리를 하는 기술들은 오늘날의 요구에 부합되게 계속 갱신되고 있다.

제39장에서는 사실자료로써 재해복구의 기본문제들을 강조한다. 주요한것은 지식 있는 정보체계보안전문가가 노는 중요한 역할이다.

제38장. 업무지속성계획화공정의 재구성

칼 비 잭슨

이 장에 대한 초판은 1999년판 《정보보안관리편람》에 서술되였다. 그때로부터 전자상업거래가 주목을 끌게 되였고 Web기반기술들이 거의 모든문제에 대한 명백한 해결방안으로 되였다. 이러한 문제들에서 일치한것은 그 경향이 어떻든 기본업무처리는 거의 변하지 않았다는것이다. 그리고 늘 그런것처럼 업무영향평가의 초점은 업무공정들에 대한 시간을 다투는 우선권을 평가하는것이다. 이러한 최근의 현실을 고려하여 이 장이 갱신되였으니 독자들이 참작해주기를 바란다.

지속성계획화: 경영진의 인식은 높지만 실행의 효과성은 낮아

지속성계획화(CP)과정이 회사의 전반적성공에 기여하는 몫을 기관이 정확히 측정하지 못하였기때문에 총적인 업무지속과정은 라선식으로 하강해 왔다. 그 하강회전 또는 분해과정은 계획작성, 검사, 유지보수, 감퇴→재계획작성, 검사, 유지보수, 감퇴→ 재계획작성, 검사, 유지보수, 감퇴 등으로 계속된다.

지난시기 연구론문 《비상사고계획화와 관리지속성계획화성능표》는 거듭하여 지속성계획화가 행정관리에 《극히 중요하다》, 《매우 중요하다》는 정도로 지위가 높아 졌다는것을 확정하였다. 가장 최근의 《2000–2001CPM/KPMG지속성계획화연구》는 이러한 관찰을 명백하게 확인하였다. 이 연구는 계속 늘어 나는 CP전문가들의 위치가 IT하부구조로부터 회사관리 및 일반관리부문으로 이동하고 있다는것을 지적하였다. 그러나 IT기관내에서의 CP보고는 여전히 기준으로 되여 있다. 현재 약 40%의 CP전문가들은 IT에 자기사업을 보고하고 있지만 30%는 자기사업을 경영진에 보고하고 있다.

지속성계획화측정

이런 추세조사가 진행되고 있지만 CP목적에 대한 행정경영진의 인식과 그들이 가치를 측정하는 방식 사이에는 서로 련관되지 못하는 점들이 계속 나타나고 있었다. 전통적으로 CP의 효과성은 메인프레임의 재해복구실험에서는 통과/불통과점수로 측정되였으며 예비/보조싸이트나 예비통신설비인 경우에는 그 CP효과성은 그 설비들에 드는 유지비와 그 설비들의 운영으로 하여 얻어 지는 리익과의 대비로 산출하였다. 이런 형식의 측정기준에서 문제점은 그것들이 단지 CP의 직접적비용을 측정하거나 또는 시험이 효과적으로 진행되였는가에 대한 간접적인식을 측정하는것이다. 이런 측정량들

은 검사가 정확한 하부구조요소를 확인하였는지 또는 구성부분을 고장날 때까지 철저히 검사하였는지 명백히 밝혀 놓지 못함으로써 그 검사환경의 범위와 리용성한계를 긋지 못한다.

따라서 우리는 리용할수 있는 정확한 측정방법에 대하여 질문할수도 있다. 재정적인 측정은 CP공정에 대한 하나의 측정량으로 되지만 CP가 기관에 기여하는 정도를 질과 효과성으로 측정하는것도 있는데 이것들은 화페로 엄밀하게 환산되지 못한다. 잘 실행되는 CP공정이 기관에 기여할수 있는것을 보면 다음과 같다.

- 계속적인 장성과 혁신
- 거래자 만족도를 개선하는것
- 사람들의 요구를 보장하는것.
- 중대한 처리과정의 질을 전반적으로 개선하는것.
- 실천적인 재정적측정을 보장하는것.

급격한 변화의 접수: CP공정의 개선

바로 천여년전부터 관리의 효률을 늘이기 위하여 전문가들은 사업능률개선과 관련한 학문들을 도입하기 시작했다. 이 학문들은 많은 산업분야와 회사들의 제조공정 및 행정업무의 전반과정을 개선하는데 서서히 도입되게 되였다. 이러한 개선노력들의 기초개념은 이러한 과정(표 38－1)이 해당 기관들에 있어서 생명력으로 되며 그것이 보다 효과적이고 효률적인 과정으로 되는 경우 오유를 크게 감소시키고 해당기관의 생산능률을 증가시킬수 있다는데 있었다.

기관의 과정들은 일련의 순차적인 활동이다. 그것이 전체적으로 실행할 때 기관사명의 기초를 구성하게 된다. 이 과정들은 기관의 하부구조(개별적업무단위, 부문, 공장 등) 전반에 걸쳐 서로 얽혀 있으며 기관의 지원구조(자료처리, 통신망, 물리적시설, 사람 등)에 매여 있다.

CP공정의 개선과 재구성움직임의 기본개념은 CP공정의 추동요인과 장애요인(표 38－1을 볼것)의 식별이다. 이 추동 및 장애요인은 여러가지 형태를 취하며(사람, 기술, 시설 등) 기관에 급격한 변화를 도입할 때 리해되고 고려되여야 한다.

앞에서 서술한 내용은 계획이 아니라 련속과정으로서의 지속성계획화에 론점을 집중하는 문제의 배경으로 된다. 지속성계획화는 기관의 중대과정들을 지원하도록 설계되여야 한다. 그러므로 이 문제는 CP에 련속고정방법을 도입하는 과정에 사람, 기술, 시설 등 추동 및 장애요인을 리해하고 취급하는데 따라 생겨 난것이다. 이것은 회복계획화가 전통적으로 검증되고 리행되던 방식으로부터 사고방식에서의 근본적이며 급속한 변화를 가져왔다.

표 38-1	정 의

활동 활동은 과정 또는 보조과정에서 진행되는것들이다. 그것은 보통 일개인 또는 한 부서의 단위로 수행된다. 활동은 보통 명령으로 문서화된다. 명령은 그 활동을 이루는 과제들을 문서화해야 한다.

성능대조 성능대조는 다른 기관들이 같은 또는 류사한 조작을 어떻게 수행하고 있는가를 연구함으로써 기관의 실지성능을 개선하기 위하여 우월한 생산과 봉사, 설계, 장비, 과정 그리고 실무를 식별하고 리해하며 창조적으로 발전시키는 체계적인 방법이다.

기관과정개선 업무과정개선(BPI)은 FAST, 과정성능검사, 과정재설계, 과정재구성과 같은 방법들을 리용하여 관리와 지원과정에서 자체기능개선이 일어 나도록 설계된 방법론이다.

비교분석 비교분석(CA)은 측정항목들을 류사한 대상에 대한 다른 측정항목과 비교하는 행위이다.

추동요인 추동요인은 과제, 활동 또는 과정의 수행을 가능하게 하는 기술적 및 기관적 편의시설/자원이다. 기술적추동요인의 실례는 개인용콤퓨터, 복사장치, 분산형자료처리, 음성응답 등이다. 기관적인 허용자의 실례는 보강, 자체관리, 통신, 교육 등이다.

고속분석해결기법(FAST) FAST는 그룹의 주의를 단일과정에 집중시키는 돌파방법이다. 그룹은 하루 또는 이틀의 회의를 통하여 다음 90일동안의 과정을 어떻게 개선할수 있는가를 결정한다. 회의가 끝나기전에 관리자는 제안된 개선안을 승인하거나 거절한다.

미래상태해결 가치를 증가시키기 위하여 연구중의 항목(과정)에 적용될수 있는 교정행위와 변화들의 결합

정보 정보는 분석되고 공유되고 리해된 자료이다.

주요과정 주요과정은 보통 기관구조안에서 여러개의 기능을 포함하는 과정이며 그 동작이 기관의 기능에 중요한 영향을 미친다. 주요과정이 너무 복잡하여 활동준위로서 흐름도를 작성하기 어렵다면 흔히 보조과정들로 분할된다.

기관 기관은 그룹, 회사, 협동체, 부문, 부서, 공장, 판매소 등이다.

과정 과정은 공급자로부터 입력을 받고 거기에 값을 첨가하며 소비자에게 출구하는 활동들이 론리적으로 련관되여 있는 순서화된(련결된) 모임이다.

보조과정 보조과정은 주과정을 지원하여 특정의 목적을 달성하는 주요과정의 일부이다.

체계 체계는 어떤 규칙적인 호상작용으로 일체화되여 기관적인 총체를 형성하는 부분품들(하드웨어, 쏘프트웨어, 절차, 인간기능, 기타자원)의 조립품이다. 그것은 련결될수도 있고 안될수도 있는 련관과정들의 모임이다.

과제 과제는 어떤 활동의 개별적요소 또는 부분모임이다. 보통 과제는 항목이 특정한 분담을 어떻게 수행하는가와 관련된다.

급속한 변화가 요구된다

경영진의 의식성은 높지만 CP실행효과성이 낮은것은 일관하고 의의 있는 CP측정이 없는것과 관련되는것으로서 그것은 회복계획화책임을 리행하는 방식에서의 급속한 변화를 요구하고 있다. 1980년대와 1990년대의 대형콤퓨터지향재해복구(DR)계획을 개발하는

데 리용된 기술은 그 방법론에 따라 5～7단계로 구성되였다. 그것은 회복계획작성자에게 다음과 같은것을 요구하였다.

1. 계획팀과 계획개발을 위한 하부구조지원을 확립하는것.
2. 위협 및 위험관리재검토를 조직하여 회복계획에서 취급되여야 할 가능한 위협환경을 식별하는것.
3. 업무영향분석(BIA)을 조직하여 시간을 다투는 업무용응용/망을 식별하고 우선시하며 최대허용고장시간을 결정하는것.
4. BIA에서 요구되는 회복우선권과 회복시기를 효과적으로 취급한 해당한 회복대안을 선택하는것.
5. 회복계획을 문서화하고 실현하는것.
6. 지속적인 검사 및 보수전략을 확립하고 도입하는것.

전통적인 재해복구계획화방법의 결함

낡은 방법은 《온실》대형콤퓨터하부구조의 재해복구가 표준으로 될 때에는 잘 동작하였다. 지어는 발전하는 분산형/의뢰기/봉사기체계들을 총체적인 회복계획화하부구조로 통합하는 경우에도 상당히 잘 동작하였다. 그러던 기관이 업무단위회복계획화와 관련될 때에는 전통적인 DR방법이 업무단위/기능회복계획을 설계하고 실현하는데서 비효률적이였다. 기업체전체범위의 회복계획을 실현하려고 할 때 1차적인 관심사는 기능적인 호상의존성에 대한 문제였다. 회복계획작성자들은 업무단위와 기능들사이의 호상의존성과 업무단위와 그 내부의 시간을 다투는 기능을 지원하고 기술봉사사이의 호상의존성을 식별하는데 사로 잡혀 있었다.

호상의존성을 장악하지 못한다

CP목적을 위하여 부서별 호상의존성을 장악하는 능력은 극히 어려우며 이를 위한 대부분의 방법들은 비효률적이였다. 여러가지 환경으로 하여 호상의존성을 계속 장악하고 있기는 어렵다. 호상의존성에 영향을 미치는 환경은 대부분의 현대기관들이 겪고 있는 급격한 변화속도이다. 여기에는 재조직화/구조조종, 사람배치, 경쟁환경변화, 해외조달이 속한다. 기관구조가 변할 때마다 CP는 변해야 하며 호상의존성이 다시 평가되여야 한다. 즉 변화가 빠를수록 CP개혁이 더디게 진척된다. 일련의 기능호상의존성이 장악되지 못할수 있기때문에 CP무결성은 상실되였으며 CP의 전반적기능은 손상되였다. 이러한 난처한 문제에 대한 답은 쉽지 않은것 같다.

호상의존성은 업무과정이다.

왜 호상의존성이 관심사로 되는가, 호상의존성이란 무엇인가. 넓은 의미에서 호상의존성은 기관의 업무과정들이며 그것들은 기관의 사명을 수행할수 있도록 작용해야 하기

때문에 관심사로 된다. 업무과정의 관점에서 회복계획화의 난점들을 대하면 호상의존성을 놓치는것과 관련된 문제들을 상당한 정도로 완화시킬수 있으며 또한 회복계획화노력의 초점을 기관의 가장 중요한 요소에 집중시키도록 할수 있다. 기관에서 시간을 다투는 업무과정들이 어떻게 구조화되는가를 리해하는것은 과정들을 업무단위/부서들로 넘길 때, 기술적인 체계들과 망, 시설, 중요기록들, 사람 등을 지원할 때 그리고 재조직화 및 변화기간의 과정들을 장악할 때 회복계획작성자를 도와 줄것이다.

지속성계획화의 공정법

메인프레임위주의 재해복구계획화에 대한 전통적인 방법은 기관의 기술적 및 통신가동환경들을 회복할 필요를 강조하였다. 오늘 많은 회사들이 기술회복으로부터 벗어나 우선권이 있는 업무과정의 지속성과 특정한 업무과정회복계획을 개발하는 방향으로 전환하고 있다. 많은 대규모협동체들은 과정재구성/개선질서를 리용하여 기관의 전반생산성을 높이고 있다. CP 그자체는 하나의 과정으로 고찰되여야 한다. 그림 38－1은 기업체범위의 CP공정구조를 어떻게 보아야 하는가에 대한 그라프적표시이다.

이러한 업무계획화방법은 다음과 같은 4가지 전통적인 지속성계획화질서를 공고화한다.

1. **IT재해복구계획화(DRP)** 전통적인 ITDRP는 집중형 및 분산형 IT능력들과 음성 및 자료통신망지원봉사를 포함하여 기관의 IT하부구조에 대한 지속성계획화요구를 취급한다.
2. **업무운영재개시계획화(BRP)** 전통적인 BRP는 기관이 자기들의 지지자원(IT, 통신망, 시설, 외부중계관계 등)에 접근하지 못하는 경우 기관의 업무운영(결산, 구입 등)의 지속성을 취급한다.
3. **위기관리계획화(CMP)** CMP는 의뢰기관이 효과적이고 효률적인 기업체범위의 비상사태/재해대응능력을 개발하도록 하는데 기본을 두고 있다. 이 대응능력은 적절한 관리진을 구성하고 그 성원들을 엄중한 회사비상사태(폭풍, 지진, 홍수, 화재, 해킹 및 비루스위험 등)에 대응하도록 훈련시키는것을 포함한다. CMP는 또한 위기나 재해대응기간에 직원들의 생명보호문제들도 포함한다.
4. **련속리용성(CA)** 우에서 설명한 기타 CP요소들과는 대조적으로 매일 24시간 매주 7일가동환경에서 하부구조지지자원의 복구시간목표(RTO)는 령시간으로 줄었다. 즉 의뢰기관은 사소한 재정적(수입손실, 추가비용) 및 운영상(거래자봉사, 신용손실) 영향을 받지 않으면 매우 짧은 시간동안조차도 운영능력을 잃어 버릴수 없다. CA봉사는 지원하부구조의 최고가동시간을 99% 또는 그이상으로 유지하는데 초점을 두고 있다.

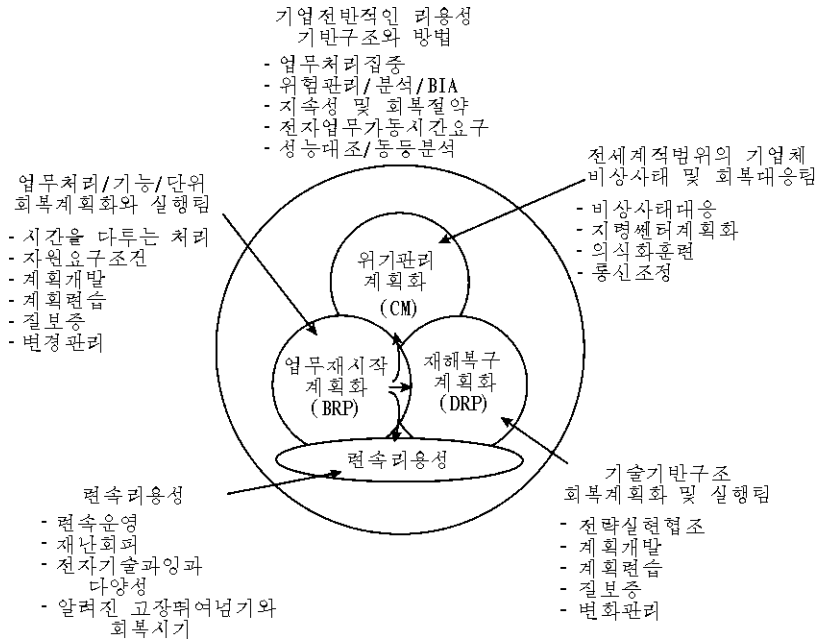



그림 38－1. 기업체범위의 CP공정구조

CP공정개선환경에로의 이행

경로도표륜곽과 고준위 CP공정방법

그림 38－2에서 보는바와 같이 CP공정을 개별적인 보조과정요소로 분할함으로써 실천적인 고준위CP공정개선방법을 검증해 볼수 있다.

6개의 지속성계획화업무과정의 기본요소를 아래에 서술한다.

현재상태평가/전진평가. 그림 38－2에서 보는바와 같은 기업체범위의 지속성계획화방법을 리해하면 지속성계획화공정의 《건강》정도를 측정할수 있다. 이 과정의 기간에 현재의 지속성계획화업무보조과정이 전체 효과성을 측정할수 있도록 평가된다. 때때로 격차분석기법을 리용하여 현재상태와 희망하는 미래상태를 리해하고 그 다음 현재상태와 미래상태사이의 사람, 과정, 기술장애요인과 추동요인들을 리해하는것이 유용하다. 그림 38－3에 현재상태/미래상태상상도를 보여 준다.

현상태평가과정은 또한 기관이 어떻게 CP공정을 평가하며 그 성공을 측정하는가를 식별하고 결정하는것을 포함한다.

흔히 세심히 관찰되지 못하면 결과 CP공정의 실패를 가져 온다. 또한 이 과정에 업무영향분석(BIA)을 통하여 전체업무에 대한 봉사손실 및 중단의 영향을 결정하기 위하여 기관의 업무과정들이 검사된다. BIA의 목적은 업무과정들에 우선권을 부여하고 그 과정들의 회복과 지원자원의 회복에 대한 복구시간목표(RTO)를 배당하는것이다. 이러한 활동

의 중요한 결과의 하나는 시간을 다루는 과정들과 지원자원들(례컨대 IT응용, 망, 시설, 리해관계 등)의 호상관계를 도표화하는것이다.

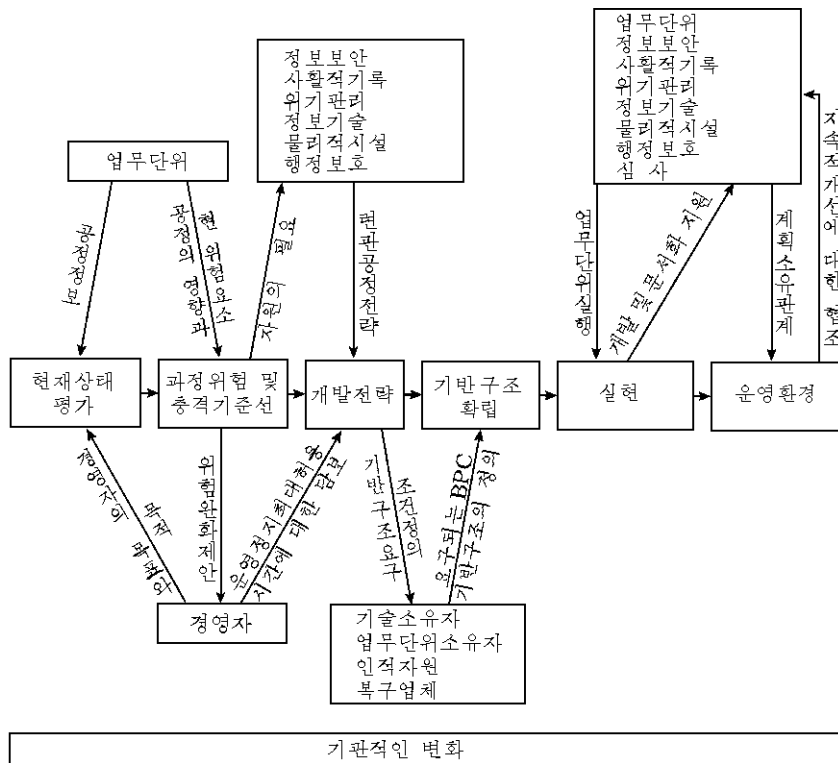



그림 38－2. CP처리개선을 위한 높은 수준의 실천적담보

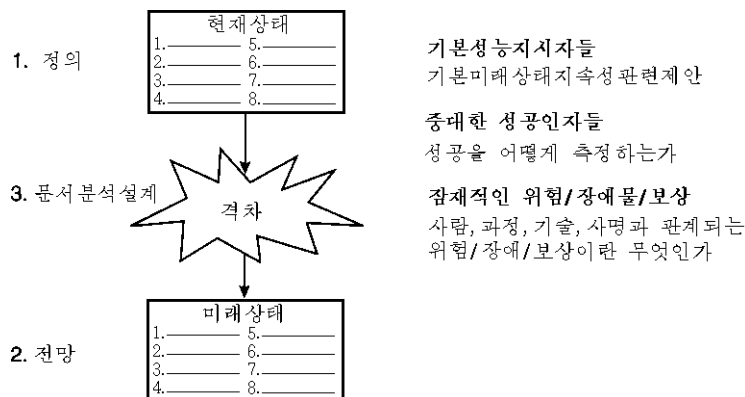



그림 38－3. 현재상태와 미래상태의 전망

과정위험과 영향기준선. 이런 과정기간에 잠재적인 위험들과 약점들이 평가되며 전략과 프로그람이 개발되여 그러한 위험들을 완화시키거나 제거한다. 독자적으로 진행하는 위험관리재검토(RMR)는 일반적으로 기관의 물리적, 환경적 및 정보능력의 보안을 검토한다. 일반적으로 RMR는 다음과 같은 분야를 식별하고 론의해야 한다.

- 잠재적인 위협
- 물리적 및 환경적보안
- 정보보안
- 시간을 다투는 지원기능의 회복가능성
- 단일점고장
- 문제 및 변경관리
- 업무중단 및 추가비용보험
- 싸이트외부의 보관계획 등

전략개발. 이 과정은 CP난문제들에 대한 가장 정확한 회복대안을 식별하고 문서화하기 위한 한번 또는 여러번의 토론회들을 가지는 과정이다(실례로 IT련속성목적으로 강력한 싸이트가 요구되는가를 결정하는것, 추가적인 통신회선이 망결합환경에 설치되여야 하는가, 추가적인 작업공간이 업무운영환경에 필요한가를 결정하는것 등). 우의 위험평가로부터 얻어 진 정보를 리용하여 장기간의 검사, 보수, 인식성, 훈련 그리고 측정전략을 설계한다.

지속성계획하부구조. 계획개발기간 모든 방책들과 지침, 지속성측정, 지속성계획은 형식적으로 문서화된다. CP환경을 구조화하여 계획소유자와 계획관리점을 식별하며 계획의 성과적인 개발을 담보한다. 또한 지속성계획을 전체 IT지속성계획과 위기관리하부구조에 종속시킨다.

실현. 이 기간에는 지속성 또는 위기관리계획의 초기변종이 기업체환경에 걸쳐서 실현된다. 또한 장기간검사, 보수, 의식화, 훈련, 측정전략들이 실현된다.

운영환경. 이 상태는 지속성 및 위기관리계획의 항시적인 재검토와 보수를 포함한다. 또한 전반적인 지속성 및 위기관리업무과정의 련속실행가능성의 보수를 필요로 할수도 있다.

어떻게 목적을 달성하는가, CP가치려행의 개념

CP가치려행은 기관의 최고경영진과 회복계획화를 책임진 사람들이 CP가능성을 공동개발하는데 도움이 되는 구조이다. 성과적이며 측정가능한 계획화공정을 달성하기 위해서는 CP가치려행의 권리과정에서 일련의 검사점들이 고찰되고 합의되여야 한다. 그 검사점들은 다음과 같다.

- **성공정의** 성공적인 CP실현은 어떤것인가를 정의한다. 미래상태는 무엇인가.
- **CP를 업무전략과 함께 세우는것** CP노력이 업무중심으로 되도록 담보하는 목표들을 대담하게 제시한다.
- **개선전략작성** 자기기관과 동료기관들이 어디에 있는가를 비교하며 동료기관에 비하여 자기의 현재 위치에 기초한 기관의 목표를 대조하고 어느 주요창안이 기관의 목적을 달성할수 있게 해줄것인가를 분석한다.
- **가속기로 되는것** 기관의 CP전략과 과정들의 실현을 가속시킨다. 오늘의 환경에서 속도는 대규모회사에 있어서 중대한 성공인자로 된다.
- **결승팀을 조직** 회사에 CP평가, 개발, 실현을 관통시킬수 있는 내부/외부팀을 조직한다.
- **업무요구평가** 지원하부구조에 대한 시간을 다투는 업무과정의존성을 평가한다.
- **계획의 문서화** 시간을 다투는 업무과정들의 리용성을 담보하는데 초점을 둔 지속성계획을 개발한다.
- **사람들을 추동** 훈련계획과 명백한 기관구조, 상세한 지도 및 관리계획 등과 같은 비상시 빠른 반응과 회복을 가능하게 하는 구조를 실현한다.
- **기관의 CP전략을 완성** 기관의 지위를 잘 타산하여 성공을 담보하는데 필요한 운영상의 그리고 인사관계의 리정표를 완성한다.
- **가치전달** 미래를 내다 보고 기관변화를 고려하는 동시에 기관의 목표를 달성하는데 집중한다.
- **갱생/개조** 새로운 CP고정구조와 기관관리에 도전하여 리용가능성과 회복가능성의 난점들을 계속 적응시키고 만족시킨다.

가치려행은 의미 있는 대화를 도와 준다

경영진의 의식성수준을 높이기 위한 이 가치려행기법은 CP공정에 대하여 의미 있는 론의를 쉽게 해주며 결과적인 CP전략이 실지로 가치를 증가시킨다는것을 담보해 준다. 후에 고찰하겠지만 이 가치증가개념은 또한 전체 CP공정의 성공이 측정될수 있는 추가적인 측정량을 제공할것이다.

기관변경관리에 대한 요구

우에서 언급한 CP공정개선방법과 CP가치려행밖에도 사람지향의 기관변경관리(OCM) 개념을 도입하는것은 성공적인 CP공정을 실현하는데서 중요한 문제로 된다.

H. James Harring ton은 저서 《업무과정개선수첩》에서 과정개선방법을 적용하는것은 흔히 기관이 변경과정을 조정하지 않는한 문제거리를 발생시킬수 있다는것을 강조하였다. 그는 이렇게 서술하였다. 《재구성과 같은 방법들은 우리가 우리의 본보기와 기관문화에 도전하고 변경시킬 때에만 성공하였다. 행동방식이나 과정을 운영하는데 책임이

있는 사람들을 변경시키지 않고 그 과정을 변경시킬수 있다고 생각하는것은 궤변이다.》.

사람추동요인과 장애요인을 식별하는것과 행동방식을 변화시키는 정확한 실현계획의 설계를 포함하여 기관변경관리의 개념은 CP계획방법을 CP공정개선으로 전환하는데서 중요한 역할을 논다. 저자는 또한 다음과 같이 지적하였다. 《고통관리, 변경계획화, 공동작용 등 변경과정을 관리하는데서 효과적인 여러가지 도구와 기법이 있다. 중요한것은 모든 업무과정개선(BPI)계획은 그 자체내에 매우 종합적인 변경관리계획을 가지고 있어야 하며 이 계획은 효과적으로 실현하여야 한다는것이다.》.

그러므로 CP공정의 개념이 기관안에서 발전하는데 따라 적당한 OCM기술이 전반적 배치사업의 필수구성요소로서 고찰되고 포함되도록 하는것은 회복계획작성자의 몫으로 된다.

성공은 어떻게 측정되는가, 채점표의 개념

CP공정의 개선방법을 더 보완하기 위해서는 기관이 전체 CP공정의 성공을 평가하는데 리용할수 있는 의미 있는 측정 또는 측정량을 확립하여야 한다. 전통적인 측정은 다음과 같다.

- 비상가동싸이트에서 얼마나 많은 돈이 소비되였는가,
- 얼마나 많은 사람이 CP활동에 전문적으로 참가하였는가,
- 비상가동싸이트검사는 성공인가.

대신에 초점은 기관의 총적목표를 달성하는데서 CP공정의 기여량을 측정하는데 집중되여야 한다. 이러한 집중에 의하여 가능한 기능들은 다음과 같다.

- 합의된 CP개발리정표를 식별하는것,
- 실행기준선을 확립하는것,
- CP공정전달의 정당성을 립증하는것,
- 경영진이 만족하여 경영사업을 앞으로도 성과적으로 진행할수 있는 기초를 마련하는것.

CP채점표는 다음의 정의를 포함한다.

- 가치주장
- 가치제안
- CP위험감소에 대한 측정지표/가정
- 실현규약
- 정당화방법

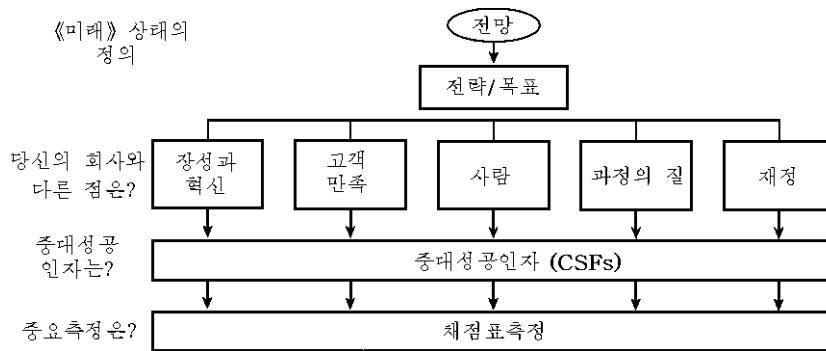



그림 38－4. 채점표개념

표 38－2 지속성과정채점표

질문 : 다음의 지속성과정요소들을 실현하는것으로부터 기관은 사람, 과정, 기술, 사명 /소득으로 환산하여 얼마나 덕을 보게 되는가

지속성망계획화공정요소	사람	과정	기술	사명/소득
과정방법론				
문서화된 DRP				
문서화된 BRP				
문서화된 위기관리계획				
문서화된 비상대응절차				
문서화된 망복구계획				
기관의 비상대응연습				
종업원의식화과정				
복구대안비용				
련속리용성하부구조				
지속성검사과정				
기타				

그림 38－4와 표 38－2는 채점표개념과 실현된 CP공정의 성공을 측정하기 위하여 개발될수 있는 측정량형태들에 대한 실례를 보여 준다. CP공정이 측정될 새로운 측정법은 이 채점표방법에 속한다.

이 채점표방법에 이어 기관은 CP공정의 미래상태가 어떻게 되여야 하는가를 정의해야 한다(앞에서 소개한 CP가치려행을 볼것). 이 미래상태정의는 기관의 최고경영진과 CP공정하부구조의 개발담당자가 공동으로 개발하여야 한다. 그림 38－3은 현재상태/미래상태상상도 즉 채점표의 예상을 개발하는데 리용될수 있는 기법을 보여 준다. 일단 미래상태가 정의되면 CP공정개발그룹은 다음과 같은 분야에서 CP공정실현의 중대성공인자의

륜곽을 그려 볼수 있다.

- 장성과 혁신
- 고객만족
- 사람
- 과정의 질
- 재정상태

이 측정은 특정한 문화와 환경에 기초하여 유일하게 개발되여야 한다.

Web기반의 응용에 대한 지속성계획화

Web과 Web관련업무의 출현과 함께 요구되는것은 가동시간 24×7시간에 대한 요구이다. 전통적인 복구시간목표들에는 기관의 Web기반을 지원하는 기업공정들과 자원들이 들어 있지 않다. 유감스럽게도 지속적인 매일 24시간 매주 7일의 가동시간에 대하여 Web기반의 응용프로그람을 간단히 준비한다면 그것은 대책으로 되지 못한다. 응용프로그람리용의 가능성문제가 취급되여야 한다는것은 명백하지만 기타 Web기반의 하부구조구성요소(콤퓨터하드웨어, Web기반의 망, 자료기지파일체계, Web봉사기, 파일 및 인쇄봉사기 그리고 이 모든것들과 관계되는 물리적, 환경적 및 정보보안상 우려에 대한 준비 등)의 신뢰성과 리용성이 담보되여야 한다는것도 중요하다. 이 하부구조전체를 치명적인 또는 부차적인 붕괴기간에 리용할수 있도록 준비한다는 말은 보통 련속 또는 고도리용성을 의미한다.

련속리용성(CA)은 간단히 이루어 지지 않는다. 그것은 조화롭게 계획화되고 실현된다. 신뢰성 있고 리용가능한 Web기반의 하부구조에서 열쇠는 하부구조의 매개 요소들이 고도의 신축성과 담보성을 가지도록 하는것이다. 이 사실을 실증하여 가트너연구소는 다음과 같이 보고하였다. 《자료기지의 복사, 하드웨어봉사기, Web봉사기, 응용봉사기, 종합중개자/묶음은 응용봉사의 리용성을 증가시켜 준다. 그러나 가장 좋은 결과는 체계의 하부구조에 대한 믿음외에 응용프로그람 그자체의 설계가 련속리용성에 대하여 고려될 때 달성된다. Web응용프로그람에 대한 련속리용성을 달성하려고 하는 사용자들은 어떤 하나의 도구에 기초할것이 아니라 응용계획의 매 단계에서 체계적으로 리용성을 고찰해야 한다.》.

련속리용성방법론을 실현하는것은 매일 24시간 매주 7일 또는 그에 가까운 리용가능성을 달성하기 위한 조직화된 방법론에서 열쇠로 된다. 이 과정을 업무과정요구와 예상, 망하부구조(례컨대 인터네트, 내부망, 외부망 등)의 약점과 위험을 리해하고 단일점고장분석을 리해함으로써 검사된다. 련속리용성의 실현을 고찰하는 일부로서 기관은 망하부구조와 그 요소들의 신속성과 하부구조관리체계의 망고장, 망구성, 망변경취급능력, 망리용성감시능력, 개별망요소들의 용량요구취급능력을 검사해야 한다. 그림 38－5는 이 방법들의 도식적표현을 보여 준다.

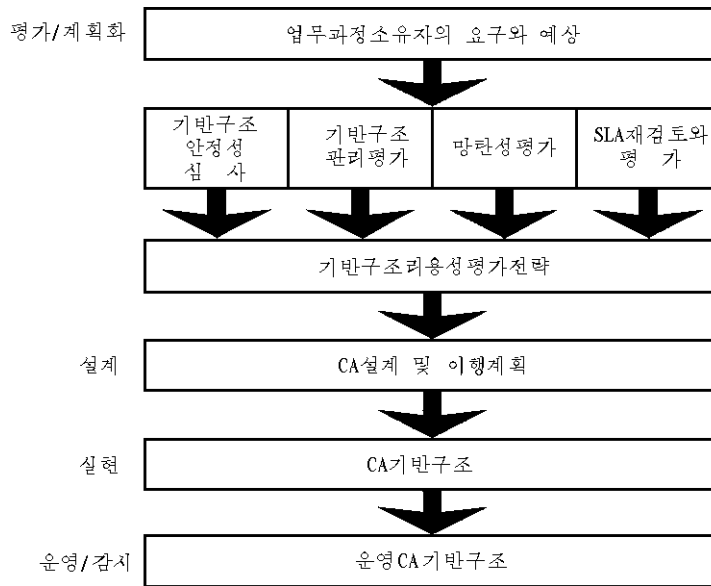



그림 38－5. 련속리용성방법론

CA방법론은 Web기반의 환경을 달성하는데서 체계적인 고찰 및 전진이동방법이다. 매우 높은 준위에서 이 방법들을 개괄하면 다음과 같다.

- **평가/계획화.** 이 상태에서 기업체는 업무과정소유자예상/요구조건과 Web기반의 업무과정을 지원하는 기술하부구조요소들의 현재상태를 리해하기 위하여 노력해야 한다. 회견기교(사람 대 사람)와 현재의 체계 및 망자동진단도구를 리용하는 것은 리용성상태와 리용성우려사항들을 리해하는데 도움으로 될것이다.
- **설계.** 현재상태평가에 대한 결과가 주어 지면 련속리용성전략과 실현/완화계획을 설계한다. 이것은 Web기반의 자원지원에 대한 접근과 리용을 승인하는데 필요한 관리과정을 분류하는데 리용될수 있는 Web기반의 하부구조분류체계를 개발하는것을 포함할것이다.
- **실현.** 설계단계에서 결정된 설계기술설명서에 따라 현재의 하부구조를 Web기반의 환경으로 완화시킨다.
- **운영/감시.** Web기반의 하부구조에 대한 전진관리를 위하여 운영상 감시기술 및 과정들을 확립한다.

이런 방향에서 마커스(Marcus)와 스턴(Stern)은 자기들의 저서 《고도리용성에 대한 면밀한 계획: 신축성 있는 분산형체계설계》에서 체계리용성을 최대로 하기 위한 몇가지 기본규칙을 권고하였다.

- **자금을 쓰되 맹목적으로 쓰면 안된다.** 질보장에는 돈이 필요하기때문에 적당한 정도의 회복능력내에서 투자가 필요하다.

- **아무것도 가정하지 않는다.** 그것이 련속리용성에 이르렀을 때는 아무것도 묶여있지 않게 된다. 종단간체계 리용가능성은 제일 선차적인 계획화를 요구하며 간단히 이루어 질수 없고 적절한 자리에 투하될수 없다.
- **단일점고장을 제거한다.** 만일 사슬에서 단일련결고리가 끊어 지면 다른 련결고리가 얼마나 강한가에 관계없이 체계는 주저앉는다. 단일고장을 식별하고 완화시킨다.
- **엄밀한 보안을 유지한다.** Web기반의 하부구조요소들에 대한 물리적 및 환경적 정보보안을 보장한다.
- **봉사기를 공고화한다.** 많은 작은 봉사기들의 기능을 보다 큰 봉사기와 많지 않은 봉사기에 집중하여 운영을 손쉽게 해주고 복잡성을 줄인다.
- **일반과제들을 자동화한다.** 일반적으로 수행되는 체계과제를 자동화한다. 운영복잡성을 줄이기 위하여 실행될수 있고 임의의것도 고도리용성을 유지하는데 도움이 될것이다.
- **모든것을 문서화한다.** 체계문서화의 중요성을 절대로 과소평가하지 말아야 한다. 문서화는 현재와 미래의 체계운영자들에게 문제시되는 체계의 근본적인 운영상 복잡성에 대한 검사흔적과 지령을 보장한다.
- **봉사준위협약(SLA)을 확립한다.** 기업체와 봉사제공자예상을 미리 정의하는것은 가장 중요하다. SLA는 체계리용성수준과 봉사시간, 위치, 우선권, 단계적확대방책을 취급해야 한다.
- **미리계획한다.** 실제적인 사건에 앞서서 비상사태와 위기, 다중고장에 대하여 계획화한다.
- **모든것을 검사한다.** 동작에 앞서 생산환경에서 새로운 모든 응용, 체계쏘프트웨어, 하드웨어변경을 검사한다.
- **개별적인 환경을 유지한다.** 가능하다면 체계들을 분리시킨다. 이 분리는 다음과 같은 기능들 즉 생산, 생산본보기, 품질보증, 개발, 실험실, 재해복구/업무지속성 싸이트에 대한 개별적인 환경을 포함할수도 있다.
- **고장분리에 투자한다.** 문제들이 발생할 때 또는 발생한다면 확대되여 다른 하부구조요소에 영향을 미치지 않도록 문제들을 분리시키는 계획을 작성한다.
- **체계의 리력을 검사한다.** 체계의 리력을 리해하는것은 체계를 앞으로 보다 높은 수준의 회복능력으로 끌어 올리기 위하여 어떤 작용이 필요한가를 리해하는데서 도움이 될것이다.
- **장성을 위하여 건설한다.** 현대콤퓨터시대에는 체계자원의 신뢰성이 시간에 따라 증가한다. 기업체가 체계자원에 더욱더 의거하는데 따라 체계는 더 커져야 한다. 그러므로 체계자원을 현재의 신뢰성 있는 체계구조에 첨가하는것은 예비계획화와 작업부담분산과 응용균일화에 대한 관심을 요구한다.
- **성숙된 쏘프트웨어를 선택한다.** Web기반의 환경을 지원하는 성숙된 쏘프트웨어가 검사되지 않은 해결방안들중에서 더 바람직하다는것은 두말할 필요가 없다.
- **신뢰성 있고 봉사가능한 하드웨어를 선택한다.** 쏘프트웨어와 같이 Web기반의 환경에서는 평균고장퇴치후 시간이 긴 하드웨어요소를 선택하는것이 더 좋다.

- **구성을 다시 리용한다.** 기업체가 안정한 체계구성을 가지고 있다면 환경전체에 걸쳐 가능한껏 많이 그것들을 다시 리용하거나 반복한다. 이 방법의 우점은 지원이 쉬운것, 미리 검사된 구성, 새로운 옮겨 보내기에 대한 고도신용, 다량구입 가능성, 예비부속품리용가능성 그리고 Web기반의 하부구조를 실현하고 운영하는것을 담당자들이 적게 학습하는것 등이다.
- **외부자원을 리용한다.** Web기반의 환경을 실현하고 운영하고 있는 기관들의 우점을 받아 들인다. 다른 경험으로부터 배우는것이 가능하다.
- **하나의 문제, 하나의 풀이.** 하부구조를 유지하는데 필요한 도구들을 리해하고 식별하고 리용한다. 도구들은 일감에 적합해야 하며 그것들이 설계되는데 따라 획득하여 리용하도록 해야 한다.
- **단순하게 한다.** 단순성은 Web기반의 하부구조를 계획하고 개발하고 실현하며 운영하는데서 열쇠로 된다. 조종, 경쟁, 변화도입에 대한 Web기반의 하부구조점들을 최소화하기 위하여 노력한다.

Maraus와 Stern의 저서는 고도로 리용가능한 체계를 준비하고 실현하는데 필수적인 참고서이다.

지속성계획화공정을 재구성하는것은 지속성계획화공정을 재활성화하는것은 물론 Web기반의 기업체의 요구와 예상이 련속리용성질서를 실현하는 과정을 거쳐 식별되고 만족된다는것을 담보하는것을 포함한다.

요 약

기관이 자기의 CP실현에 대한 성공을 측정하지 못한다면 계획개발과 감퇴의 끊임없는 순환이 진행된다. 그 첫째 리유는 정확한 CP측정수법들이 기관의 미래상태목표에 알맞게 도입되지 못하였기때문이다. 이런 측정수법들이 없는것으로 하여 최고경영진과 CP담당자들의 예상은 흔히 충족되지 못한다. 《비상계획화와 관리/KPMG지속성계획화 연구》에서 수집된 통계자료는 이러한 주장을 립증해 주고 있다. 이에 기초하여 기관이 CP실현을 담당하는 방식의 급격한 변화가 필요하다. 이 변화는 CP에 대한 업무과정개선 (BPI)방법을 도입하고 리용하는것을 포함한다. 이 BPI방법은 지난 20년동안 《포춘》잡지에 오른 1000여개의 최우수회사들에서 성과적으로 실현되였다. CP를 한개 과정으로 정의하며 CP가치려행의 개념을 적용하며 CP채점표를 리용하는 CP측정을 확장하며 기관변화관리(OCM)개념을 련습하는것은 CP에 대한 극히 각이한 방법을 손쉽게 해줄것이다. 마지막으로 Web기반의 업무과정들이 24×7가동시간을 요구하기때문에 련속리용성질서의 실현은 CP공정이 가능한껏 충분히 개발되도록 하는데 필요하다.

참 고 문 헌

1. *Contingency Planning & Management,* January/February 2001. (The survey was conducted in the U.S. in October 2000 and consisted of readers and respondents drawn from *Contingency Planning & Management* magazine's domestic subscription list. Industries represented by respondents include Financial Services; Manufacturing/Industrial, Telecommunications, Education, Utilities, Healthcare, Insurance, Retail/Wholesale, Petroleum/Chemical, Information/Data Processing, Media/Entertainment; and Computer Services/Systems.)
2. Harrington, H.J., Esseling, E.K.C., and Van Nimwegen, H., *Business Process Improvement Workbook*, McGraw-Hill, 1997.
3. Harrington, p. 18.
4. Harrington, p. 19.
5. Robert S. Kaplan and David P. Norton, *Translating Strategy into Action: The Balanced Scorecard,* HBS Press, 1996.
6. Harrington, p. 1-20.
7. Gartner Group RAS Services, COM-12-1325, 29 September 2000.
8. Marcus, E. and Stern, H., *Blueprints for High Availability: Designing Resilient Distributed Systems,* John Wiley & Sons, 2000.

제３９장. 업무재개의 계획화와 재해복구: 사실자료

케빈 헨리

업무재개와 재해복구의 계획화는 아마도 정보보안에서 쉽게 빠뜨리거나 뒤로 미루어 놓는 부분일것이다. 업무재개계획을 준비하기 좋아하는 사람은 아마 별로 없을것이다. 보험에서와 같이 기대를 거는것이 결코 필요해서 그런것은 아니다. 그리고 이러한 문제들은 엄밀하지 못한 과학이기때문에 정확히 완성되였다는것을 확정하기가 매우 어렵다. 그러나 흔히 누구도 업무재개계획화를 고의적으로 지연시키지는 않는다. 이러한 문제들은 다른 일감부하 그리고 비용, 시간과 같은 다른 제약조건, 표면상 더 긴급한 과제들로 인하여 해결되지 못할뿐이다.

모든 회사들중 50%미만이 자기 실정에 맞는 신뢰성 있고 완전하며 현실적인 업무재개 및 재해복구계획을 가지고 있다. 때문에 많은 회사들은 사활적인 업무재개계획의 결여를 보충하기 위하여 두개의 방안을 고려하고 있다. 첫번째 방안은 회사안에서 위험관리자의 직무 즉 업무재개와 재해복구계획을 조정할 1차적인 책임을 가지는 직무를 두는것이다. 두번째는 매 개발과제에 업무재개 및 재해복구계획자금투자와 시간일정을 작성하는것이다. 이것은 개발과제에 착수하여 팀의 성원들을 분산시키기전에 계획개발을 촉구할것을 목적으로 하고 있다. 이 방안들의 효과성은 개발과제종결전에 위험관리자의 역할과 과제완성을 조정하는 상급경영진의 지도에 크게 관계된다.

기관들은 업무운영의 부분적인 또는 전체적인 중단을 실지로 체험하는것을 바라지는 않는다. 이러한 체험과정에는 괴로움도 있지만 즐거움도 있다. 재해복구를 체험한 회사는 장기간의 업무운영에서 리득을 볼수 있는 잠재력을 가지게 될것이다. 이 장은 콤퓨터체계고장의 실지 사실자료와 재난으로 되는 사건들을 검토한다. 이 특이한 사건들에서 업무계획은 실시되였지만 언제나 그러하듯이 그것이 완성된 해결방도는 아니였다. 그러나 업무계획이 수립됨으로써 그것을 기준으로 하여 업무공정을 계측하고 기업운영을 계속해 나갈수 있었던것이다.

업무재개계획은 《정상》과정이 파괴되는 사고에서도 업무운영을 계속할수 있는 다른 방법을 보장할수 있게끔 설계되여야 한다. 업무재개계획은 또한 업무과정을 파괴시킬수 있는 모든 형태의 경우를 다 취급해야 한다. 파괴는 콤퓨터고장일수도 있지만 대체로 보통의 업무운영을 방해하는 내부 및 외부사건들에 의한것이다. 기타 다른 파괴들은 화재, 홍수 등의 환경적인것일수 있으며 또한 작업중단, 가스루출, 전원사고 등의 외부적인 요인일수 있다. 자료처리싸이트에서 얼마간 떨어 진 곳에서 급수관이 파괴되는것도 주목할만한 콤퓨터체계고장요인이다. 공기조화장치에 물공급이 중지될 때 공기조화장치는 차단되며 자료쎈터는 순식간에 과열된다.

업무재개계획 및 재해복구계획의 1차적인 목적은 재해발생가능성을 줄이는것이다. 이것은 정확히 작성된 업무재개계획의 초기단계의 본질적인 산물이다. 업무재개팀이 계획을 개발하려는 분야를 검토한다면 체계 또는 회사가 직면한 위험을 알수 있게 된

다. 이렇게 되면 또한 운영고장을 일으킬수 있는 약한 고리를 포착하고 식별할수 있다. 이 약한 고리는 체계, 처리과정, 하드웨어, 쏘프트웨어, 숙련부족, 예견하지 못했던 인사문제에서 발견될수도 있고 환경 또는 외부위협형태로 발견될수도 있다. 계획의 목적은 다음으로 업무공정의 기반을 마련하여 다른 방법으로 기업의 정상운영을 재개하는것이다. 업무재개계획의 실현속도는 1차적으로 체계의 중요성에 의존한다. 중요한 체계(병원, 비행관제 등)는 몇초 또는 몇분안으로 동작할수 있도록 계획을 세워야 하며 그리 중요하지 않은 체계는 수일 지어는 수주일동안 천천히 동작상태에 이르도록 계획을 세울수 있다. 성공적인 업무재개씨나리오에 대한 좋은 실례로는 1999년에 3주동안 운영관제쎈터를 페쇄시킨 화재에도 불구하고 운영을 계속 진행한 유나이티드 애어라인즈항공회사의 능력을 들수 있다. 그 싸이트에서는 하루에 2,500여회의 비행을 관제하고 있었지만 이 회사는 한 시간도 안되여 후원싸이트에서 처리를 다시 시작할수 있었으며 결과 한번의 비행이 취소되고 몇번의 비행이 조금 지연되였을뿐이였다. 다행히도 이 후보싸이트는 새로운 업무재개계획의 개발부분으로서 도입검사의 마지막단계에 있었던것이다.

일단 재난이 들이 닥치면 업무그룹의 1차적인 목적은 가능한껏 중요한 체계에 운영상 영향을 주지 않으면서 운영을 재개하며 동시에 재해복구계획을 실현하는것이다. 재해복구계획의 1차적인 목표는 한도이상의 손해를 방지하는것이다. 이것은 최우선적인 목적으로 개인의 안전을 담보한다는것을 의미한다. 재해복구계획은 새 분야 즉 손상된 싸이트의 정리(페품수집 및 수리), 예비업무운영의 지원, 정상과정에로의 이행으로 갈라 진다.

업무재개 및 재해복구계획의 최종목표는 업무운영이 정상 또는 재난이전상태로 다시 시작할수 있을 때 달성되게 된다. 제때에 운영을 회복하거나 재개할수 없다면 그것은 전체 업무고장의 약 50%라는 파괴적인 통계값을 초래한다.

업무재개 및 재해복구계획이 효과적인것으로 되자면 완전히 문서화되여야 한다. 모든 책임과 과제, 쏘프트웨어와 하드웨어, 통신회선들, 보안요구조건들이 문서로 작성되여 요구될 때 즉시 리용할수 있어야 한다. 재난이 일어 난 다음에 업무운영에 대한 풍부한 경험과 리해를 가지고 있는 직원들과 상담하여 업무재개를 계획하는것은 충분한것이 못된다. 정확히 문서화되면 누구든지 그 문서를 읽고 동일한 결론을 내리고 동일한 작용을 수행할것이다. 바로 이렇게 될 때에만 문서화가 철저히 그리고 명백히 진행되였다고 할수 있다.

사실자료

이 사실자료는 Serv–co(가명)가 체험한 실제적인 사건들이다. 이 재난으로부터 배우게 되는 정보량은 아주 방대하다. 즉 재난을 일으키고 재난에 기여하는 사건들의 순서를 고찰함으로써 그 재난을 조종할수 있는 경험을 배울수 있다.

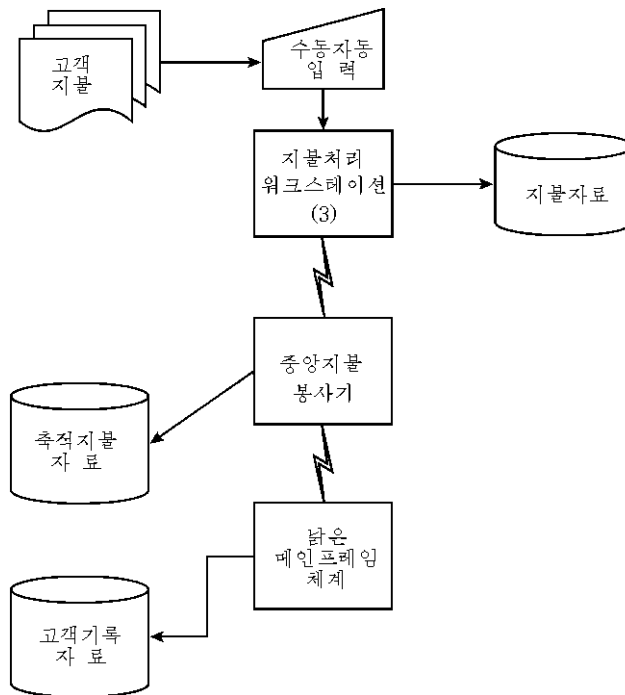



그림 39－1. 지불체계배치도

Serv–co는 회사의 수입지불전체 즉 인터네트우편지불검사 그리고 자체은행과 독자적인 대리점 및 대표부 등 Serv–co의 대리점들이 취급하는 지불처리체계(그림 39－1)를 가지고 있었다. 지불처리체계는 매일 25,000건이상의 지불을 취급하였다. 이 수입지불은 세개의 워크스테이션에서 취급되였다. 워크스테이션조작수들은 지불량과 계산수자를 워크스테이션에 입력시킨다. 일단 천건의 지불이 입력되면 그 파일은 닫기며 중앙봉사기에 전송된다. 파일에 조종이 부여되면 파일의 무결성과 오유탐지를 협조한다. 지역관리자는 하루에 한번씩 봉사기에 등록하며 그날의 처리파일을 다 하나의 큰 파일로 묶는다. 예비적인 장부처리가 이루어 지면 관리자는 모든 고객구좌관리와 송장작성을 취급하는 낡은 메인프레임체계와 통신회선을 확립한다. 관리자는 그 메인프레임에 축적파일을 전송한다. 일단 대형콤퓨터체계가 수신하면 모든 지불활동을 개별적인 고객구좌들에 공시하는 묶음처리가 실행되였다.

유감스럽게도 어느날 지불처리체계가 고장났다. 모든 고장이 그러하듯이 많은 사람들의 마음이 이미 해변가에 가 있는 한 여름철 금요일 오후에 지불처리체계에 고장이 발생하였다. 지역관리자는 지원제작업체에 전화를 걸어 그날 지불총계파일을 대형콤퓨터체계에 전송하려고 할 때 이상한 오유코드가 나왔다는것을 알렸다.

메인트그룹(Maint Group)이라는 지원회사는 월요일 아침에 Serv–co에 나와서 문제를 조사하고 바로 잡겠다고 금요일 밤에 합의하였다. 회사는 심중한 문제가 아닌것으로 생각하였다. 지난 시기에 약간의 체계고장이나 파일오유불균형으로 고객들의 구좌에 대한 지불공시가 하루이틀정도 지연되는 일이 드문히 있었던것이다.

월요일 아침 일찌기 메인트그룹의 기술자가 좋은 기분으로 도착하여 인사교환이 있었다. 메인트그룹은 그 장비의 본래제작업체가 아니였다. 즉 메인트그룹은 원래의 제작업체가 업무를 중단했을 때의 보수계약의무를 맡고 있었다. 그 기술자의 안색은 순간적으로 흐려 졌다. 그는 이 장비에 대하여 수년간의 경험을 가지고 있지만 결코 이러한 오유상태는 겪어 보지 못하였다는것을 인식하였던것이다. 이 시점에서 사무망과 제2부류지원그룹을 가진 그 대규모제작업체의 가치는 명백해 졌다. 이것은 일반적오유가 아니였으나 그 기술자는 다른 분야와 접촉하여 도움을 받을수 있었다(표 39－1을 볼것).

표 39－1　　　　　　　　　　제작업체의 선택

하드웨어나 쏘프트웨어를 새로 구입할 때 또는 회사내지원과 외부보수계약합의를 판단할 때 제작업체의 선택은 매우 중요하다. 선택할수 있는 회사의 수는 제한되여 있으며 특히 독립적인 제품들을 포함하고 있을 때 더욱 그러하다. 그러나 가능한 회사나 대리점이 기초적인 갱신과제들을 수행하고 감독할수 있게 자체로 충분한 기술을 유지하도록 해야 한다. 이것은 제작업체의 실수나 제작업체의 로동분규에 대처한 보호수단으로 된다. 또한 대규모제작업체를 선택하는것은 국부적인 작은 제작업체를 선택할 때보다 더 많은 비용이 들수도 있다.

제작업체가 클수록 보다 많은 비용으로 보다 많은 기술과 장비의 지원을 제공할수 있으며 보다 작은 제작업체일수록 보다 빠르고 개인적인 준위의 봉사를 제공할수 있는것이다. 그 제작업체가 추상적인 또는 주문문제들을 취급할수 있도록 적절한 위치에 적당한 지원체계를 가지고 있는가와 예비요소들에 접근할수 있는 준비가 되여 있는가를 재검토한데 기초하여 제작업체를 선택하여야 한다. 이때 그러한 지원을 위하여 보다 많은 비용이 들수 있으며 재난환경에서 그것은 중대한것으로 된다.

오유는 하드디스크의 고장이며 하드를 교체해야 한다는것이 판명되였다. 여기서 Serv–co 지불처리체계의 기본결함이 명백해 졌다. Serv–co는 체계를 구입할 때 봉사기급의 장치를 구입할 대신에 하나의 하드구동기와 하나의 전원만을 포함한 체계봉사기를 구입하였다. 이로 하여 Serv–co자체의 정보체계표준그룹은 체계의 보수와 감독을 맡을것을 거부하였다.

처음에 구입할 때부터 지불처리그룹은 또한 새로운 위치에 옮겨 졌다. 이것은 그들의 워크스테이션과 봉사기가 새로운 시설로 이동한다는것을 의미한다. 장비들이 안전한 방에 위치하였지만 적당한 전원공급이 보장되지 않았으며 적당한 환경조건도 보장되지 않았다. 봉사기자체도 탁상과 같은 선반에 설치되였다. 더우기 여벌테프를 위한 안전하고 조직화된 기억설비도 보장되지 않았다. 지불처리작업그룹은 콤퓨터에 커다란 흥미를 가지고 장비를 다루는데서 아주 열성적인 몇명의 직원들을 가지고 있었으나 그들은 알맞춤한 훈련이나 지식이 없었고 체계설치에서의 일부 기본적인 결함을 식별할수 없었다.

많은 회사들과 마찬가지로 Serv–co는 몇년전에 몇가지 기본적인 구조조정을 진행하였다. 그 일부로서 체계에 대하여 가장 잘 인식하고 있는 몇명의 종업원을 정리해고안에 따라 Serv–co에서 내보냈다. 체계에 대한 문서화는 거의 없었거나 완전히 없었기때문에

체계에 대한 실지 지식은 그들과 함께 많은 량이 없어 지게 되였다(표 39－2를 볼것).

표 39－2 문서화

문서화는 아마도 재난대응책으로서 가장 중요한 자원인것 같다. 그것이 정확히 준비된다면 모든 직원들이 자기들의 과제와 책임을 리해하고 그 과제가 재난속에서 다른 활동들과 어떻게 련관되는가 하는것을 리해할수 있다. 리상적으로 문서화는 명백히 표준형식으로 진행되여 문서의 흐름을 리해하는데 시간과 노력이 들지 않게 해야 한다. 이것은 그 문서를 읽는 사람은 다 같은 결론을 내리고 같은 작용을 수행한다는것을 의미한다.

문서화는 체계주위의 모든 과정들과 과제들에 대하여 특히 루틴이나 사소한 일상 과제들에 대하여서도 진행되여야 한다. 흔히 그것은 전문가들만이 할수 있는 과제이다.

다시 사실자료로 돌아 가자. 그 기술자는 이제 봉사기를 위한 새로운 하드구동기를 구해야 한다. 장비는 12년이상 오랜것이기때문에 그것은 구식이며 매 부분품들은 구하기가 아주 힘들게 되였다. 사실상 메인트그룹은 2년전에 통고를 보내면서 이 체계의 하드구동기는 제작자가 계속 생산하는것이 아니며 예상수명을 초과하였다는것을 지적하였다. 메인트그룹은 즉시 장비를 교체할것을 권고하였다. 이 충고와 함께 메인트그룹은 또한 이러한 제한성으로 하여 《최선을 다하여》 그 장비들을 계속 지원해 줄수 있을뿐이라고 지적하였다.

그 기술자는 다른 도시에서 하드구동기를 찾을수 있었으며 다음날 (화요일) 아침일찍 Serv–co에 보내줄것을 합의하였다.

화요일 아침 짐함이 도착하였으나 그안에 들어 있는 구동기는 짐함걸면에 표시된것과는 다른것이였다(명백히 이러한 중요한 송달이 요구될 때에는 언제나 발송자가 송달내용물을 검증하는데 필요한 단계를 취해야 한다).

이 시점에서 Serv–co는 사소한 고장으로부터 기본재난으로 이행하기 시작하였다. 날이 감에 따라 Serv–co에 지불하는 고객의 수가 늘어 나고 그들은 지불에 응하지 못한다는 통지를 받게 되였다. 더우기 이 통지는 거래자들에게 부당한 지연지불부담을 할당한다. 이것은 고객봉사대표부들에게 작업부담을 증가시켰으며 가난한 고객들의 신고와 나아가서 대중보도계에 불쾌한 여론을 일으켰다. 결국 이 재난으로 15,000명이상의 고객들이 피해를 입었다.

메인트그룹은 온 나라를 뒤져서 하드구동기를 두개 더 찾아 냈으며 다음날 아침에 Serv–co에 송달하도록 합의하였다. 그러나 수요일아침에 송달이 진행되지 못하였다. 정기항공로의 파괴로 하여 비행이 취소되였으며 그 짐함은 결국 도착하지 못하였던것이다.

목요일 아침에 다행히도 대체품하드구동기가 도착하였다. 기술자는 안심하고 그것을 설치하기 시작하였다. 다 설치한 다음 기술자는 새 구동기에 조작체계를 적재하기 위하여 지역관리자에게 체계복사본을 요구하였다. 관리자는 책상우의 당반에서 낡은 테프통을 꺼내 기술자에게 넘겨 주었다. 그룹에서 콤퓨터지원인원들을 축소한 이후로 몇년동안 관리자는 성실하게 예비파일들을 취하여 이 테프에 기억시키고 있었다. 그가 알지 못하

고 있었던것은 자기가 보관해 놓은 모든것이 조작체계가 아니라 일상적으로 쓰는 거래파일들이였다는것이다. Serv–co는 조작체계의 중요한 예비복사본을 가지고 있지 못하였다.

메인트그룹기술자는 자기의 기술집단에 전화를 걸어 조작체계의 일반 복사본을 리용할수는 있으나 본래제작업체(기억하고 있는바와 같이 업무를 중지하였다)가 조작체계에 설치하였던 특정한 요구는 실현될수 없다는것을 알게 되였다. 이 일반복사본이 설치되였으나 현재 상태로는 리용할수가 없었다. 메인트그룹은 즉시에 Serv–co응용의 요구에 맞게 조작체계에 수정을 가하기 시작하였다. 이 수정본은 다음주 목요일에 준비된다고 약속되였다.

이 단계에 와서 고객들에게 주는 영향이 사활적인것으로 되였기때문에 Serv–co는 자기의 업무지속성프로그람을 검토하기 시작하였다. 정확한 프로그람이 그러하듯이 그것은 위험시간인자를 반영하였으며 이 그룹에 적용되였다. 관리자는 지불처리가 Serv–co에 의하여 제공되는 기타 일부 봉사들만큼 중대하지 않다는것을 고려하여 업무과정이 다시 시작되기전까지 며칠간 지연될수도 있게 계획을 설계하였다. 업무재개계획은 지불들을 재정통계계산프로그람에 수동적으로 입력시키는 방법으로 계획되여 있었다. 이 통계프로그람은 낡은 메인프레임체계와 FTP로 련결되여 있었으며 묶음처리는 새로운 파일들을 읽는데 적용할수 있었다. 이것은 방대한 로동집약형운영이였으며 Serv–co안의 각 부서들에 지령이 떨어 져 이 지불들을 입력시키기 위하여 직원들이 오래동안 주말휴식기간에도 작업하게 되여 있었다.

수동적인 작업이 진행되기때문에 완성된 통계프로그람에서 오유를 탐지하는데 보다 많은 직원들이 요구되였다. 사실 창조된 많은 통계프로그람에서 단 한개만이 오유가 없는것으로 판정되였다. 지역지불처리관리자는 위험관리그룹을 호출하여 업무지속성계획실현에 대하여 경고를 주었는데 오히려 자기 직무에 전념하라는 충고를 받았다. 이것은 위험관리그룹의 역할에서 파멸적인것으로 되였다. 위기관리 및 과정흐름에 대한 지식과 인사과, 법률과, 회사통신과 등과 같은 다른 그룹들과의 친밀성으로 하여 그들은 이 재난을 처리하는데서 실질적인 협조를 보장할수 있었다. 그러나 많은 부서들과 같이 위험관리부는 휴가로 하여 인원이 부족되였다. 이와 같이 협조와 지원이 없었으므로 지역지불처리관리자는 곧 다른 그룹으로부터의 운영예정과 회복에 대한 호출로 하여 당황하게 되였다. 관리자와 그룹의 기타 사람들의 시간상요구는 업무요구에 대한 응답능력에 더욱더 영향을 주었다. 위험관리부로부터 자료를 받지 못한데 대한 다른 결과는 로조단체들과 정확한 련계가 이루어 지지 못한것이며 회복노력을 위하여 지원을 받을 대신 관리자가 또 다른 로조단체들로부터 직원문제에 대한 몇가지 불만건에 직면한것이다.

이것은 로사관계의 전반 풍조에 따라 피할수 없는것이였다. 로조와의 련계를 옳게 가졌더라면 이미 조성된 팽팽한 환경속에서도 더이상 악화되지 않았을수도 있었을것이다.

화요일아침 메인트그룹기술자는 조작체계수정본을 가지고 도착하였다. 그것을 설치하자 수정본은 몇가지 기능을 제공하였지만 오유탐지와 장부처리기능의 많은 부분이 결핍되게 되였다. 또한 봉사기는 메인프레임과 통신회선을 확립할수 없었다. 후에야 회선이 설치되였는데 그것은 두 기술자가 3일에 걸쳐서 진행하였다. 역시 문서화가 제대로 진행되지 못하였으므로 중요한 정보부분을 놓쳤던것이다. 다행히도 몇달전부터 통신회선목록

을 작성하고 있던 LAN지원자에 의하여 구성복사본이 휴지통에서 발견되였다.

그 다음주에 Serv–co는 자기의 지불처리를 진행할수 있었으나 인력과 신용에서 많은 비용이 들었다.

고장시에 Serv–co는 이미 교체체계를 샀으나 제작업체가 아직 그것을 송달하지 못하였다는것은 주목할만한것이다. 이 과정은 구식장비라는것이 판명된 2년전부터 시작되였다. 그러나 그것은 로상에서 몇가지 장애에 부딪쳤다. 관리부는 두번이나 지불처리부서에 구입제안을 보냈고 다른 방안(해외구입)과 보다 비용이 적게 드는 대책을 제기하였다. 이것은 교체를 오래동안 지연시켰으며 결국에는 현재의 장비가 고장나게 되였다.

또한 지불처리지역은 정보체계표준그룹의 조언을 받지 않고 교체체계를 구입하였다. 결과 새 장비는 낡은 장비와 비슷하게 한개의 하드구동기와 한개의 전원을 가지고 있었다. 그것은 또한 단독체계로 설계되였으며 계획은 련합기업체기억체계의 후원을 받도록 작성되지 못하였다. 실지로 정보체계표준그룹은 다시 한번 그것이 새로운 체계를 지원하지 못할것이며 개발과제와 관계되는것은 오직 유산체계에 대한 결합부가 정확히 동작할것이라는것뿐임을 선언하였다.

결국 Serv–co는 이 재난으로부터 무엇을 배우게 되였는가, 독자들은 무엇을 배울수 있는가, 아마 많을것이다.

전문가지원

모든 체계들은 정보체계(IS)전문가의 감독하에서 설치되며 회사표준에 따라 진행되도록 해야 한다. 단독체계의 조달 및 지원에서 IS측과 적극적인 련계를 가지는것은 많은 사소한 오유들이 중대재난으로 넘어 가지 않게 해줄수 있다. 만일 회사가 표준을 자체로 개발하지 않는다면 비호환성장비들을 통하여 보안하부구조에서 발생하는 그이상의 결함들을 방지하게 될것이다. 장비가 더욱더 표준화될수록 자체의 지식으로도 정확한 조작체계수정본을 최신판으로 보다 쉽게 유지할수 있다. 표준장비는 또한 부하공유를 더 쉽게 해주고 단일고장점을 최소화해 준다. 이를 위하여 모든 회사들은 자기들의 모든 체계에 대한 지능적인 지원을 확보해야 한다. 특히 체계가 외부계약자에 의하여 개발될 때에는 체계에 대한 지식이 그 개발과제에서 빠지지 않도록 해야 한다. 재난이 해소된 다음 Serv–co의 지불처리와 IS부서는 협동하여 교체체계를 다시 설계하기 시작하였다. 여기에는 기업체기억체계후원과 봉사기급의 장비구입이 포함되여 있었다.

예비본

모든 조작체계들에 대하여 정확한 예비본이 있어야 한다는것은 두말할 필요가 없다. 흔히 그것은 자칫하면 빠뜨려 놓을수 있는 구성(통신, 경로기 등)과 규칙기지(방화벽)이다. 모든 경우에 예비본은 처리주기가 필요하다면 다시 구성될수 있다는것이 충분히 담보되도록 진행되여야 한다. 체계가 어떤 파일들을 2차 또는 3차로 유지하는 경우에 대한

실례는 많다. 고장이 발생하면(특히 고장이 응용프로그람변경에 관계될 때) 프로그람작성자는 그 과정을 다시 실행시켜 보아야 한다. 만일 재실행이 실패하면 그 예비본은 이미 낡았다고 보고 문제를 교정하기전에 지워 버리는 일이 있을수 있다. 재정기록에 대한 장기간의 보유와 같이 예비본에 대한 모든 요구가 만족되도록 하는것이 또한 중요하다.

오늘날에는 여러가지 테프 및 CD를 비롯하여 각이한 형태의 예비본매체들이 있다. 최근의 CD문서화는 불리한 조건에서도 200년까지의 수명은 문제로 되지 않으며 난문제는 암호화열쇠가 안전하게 보관되도록 하는것과 CD를 읽는데 필요한 쏘프트웨어가 요구될 때마다 리용가능하도록 하는것이다.

예비본은 기록할 때에는 항상 예비복사본을 읽기가능하도록 해야 한다. 어느 한 회사는 최근에 디스크자두쓰기고장으로부터 회복을 시도하다가 새로 구입한 20개 테프들중 4개가 고장이라는것을 발견하였다. 예비본으로부터 회복할 필요가 있는 시점에서 예비본이 고장난다면 문제의 범위는 지수적으로 확장된다.

설비로화

지금 회사들과 대리점들에서 리용하고 있는 많은 장비들은 이미 자기 수명을 초과한 것들이다. 특히 하드구동기, 전원, 테프인 경우에 더욱 그러하다. 모든 설비에 대하여 규정대로 목록을 작성하고 설비명세를 재검토하여 그것이 여전히 신뢰성 있도록 해야 한다.

의존성

많은 체계들과 업무과정들은 거기에 의존하고 있는 다른 체계들에 대하여 인식하지 못하고 있다. 또 그것들자체가 처리를 위하여 의존하고 있는 체계들을 알지 못하고 있다. 내부 및 외부체계의존성을 전부 보여 주는 상세한 흐름도를 작성하여 체계가 고장나는 경우 그것이 다른데 영향을 미친다는것을 즉시 나타 내도록 해야 한다. 이것은 통제를 받아야 하는 재정체계와 재정부문에서 특히 중요하다. 여기서는 한개 파일이 빠지면 눈에 크게 띄지 않을수 있으나 처리 또는 법적처벌에 큰 영향을 미칠수 있다.

암호화

체계가 어떤 암호화형식을 가진다면 회복을 위하여 모든 열쇠를 안전한 장소에 보관하는것이 필요하다. 흔히 체계가 얼마동안 동작하고 있으면 열쇠는 잊어 버린다. 체계가 고장을 일으킬 때 열쇠를 알지 못한다면 그것은 극히 위험한것으로 된다. 직원이 회사문서나 파일에 대하여 암호화를 리용할 때에는 반드시 열쇠사본이 안전하고 믿음직한 장소에 보관되여야 한다. 지금까지 사고나 퇴직으로 직원이 없어 진것으로 하여 회사가 중대파일을 회복할수 없게 된 일들이 많이 일어 났다. 최근에 어느 한 회사에서는 부정행위로 하여 퇴직당하게 된 직원이 자기열쇠와 몇개의 중요체계에 대한 관리통과암호를 내놓기를 거절함으로써 회사에《인질》로 잡힌 일이 있었다.

제작업체고장

모든 정보처리분야에서 가장 보편적인 특성의 하나는 제작업체의 변경일것이다. 거의 매일이다싶이 제작업체들은 문을 열고 닫고 합쳐 지며 업무방향을 변경시키고 있다. 이렇게 기술을 보다 새로운것으로 빨리 교체하는것으로 하여 업무재개계획은 일정한 영향을 받고 있다. 정보체계전문가들은 자기들의 제작업체지원망의 상태를 계속 알고 있어야 한다. 제작업체전화번호목록과 접촉목록은 업무재개계획에 함께 유지되여야 하며 많은 계획들에는 주요고장사고에서의 우선권에 기초하여 새로운 장비를 공급하도록 제작업체들로부터의 약속도 포함되여야 한다.

제작업체가 공급한 쏘프트웨어는 신용이 담보된 3자에게 보관되여 제작업체가 그 유지를 만족시킬수 없거나 계약상조건을 갱신할수 없는 경우에 리용할수 있도록 되여 있어야 한다.

새로운 장비를 구입할 때 위험한것은 항상 그것이 계속 생산되며 지원될것인가 아닌가 하는것이다. 일련의 회사들은 최근에 구입한 장비들에 대하여 보수합의를 얻을수가 없었다. 왜냐하면 제작업체들은 새로운 업무방향으로 이동하였으며 어떤 제품계렬은 포기하였기때문이다.

제작업체를 선택할 때 대규모의 지원망과 여유장비리용가능성을 가지고 있는 높은 가격의 제작업체를 택할것인가 아니면 보다 작고 지역적인 제작업체를 택하고 여유부분품을 구입하며 자체의 전문가집단을 크게 꾸리는것으로 위험을 완화시키겠는가 하는 판단을 내려야 한다.

BCP의 갱신

종합적이고 완성된 업무재개계획을 설정하는것은 어려운것이지만 계획설정으로 완성되는것은 아니다. 회사, 부서, 기관은 여전히 끊임없는 갱신을 위하여 앞선기준에서 계획을 책임진 사람을 선정해야 한다.

계획은 적어도 1년에 한번 그리고 부서구조가 크게 변화되는 경우에 다시 검토되여야 한다. 이 책임은 업무재개계획을 유지하고 공동위험관리팀에 부서를 대표할 사람의 직능규정으로 밝혀 져야 한다. 만일 부서가 일상적으로 일감을 재검토한다면 이 책임고수문제는 재검토되여야 한다.

로 동 조 합

오늘날 로동조합은 많은 회사들에서 현실적으로 존재하며 그것으로 하여 종업원들과 경영자들은 일련의 법적인 제한조건들을 준수해야 한다. 법률적인 견지에서 로조의 성원인 어느 개인과 따로 합의를 교섭하는것은 비법이다. 위기가 오면 흔히 경영자들은 개

별적인 지불이나 보상을 종업원들과 직접적으로 교섭하려고 시도해왔다. 이것은 현실성 있는듯하지만 이것 역시 위법이다. 업무재개계획에는 업무중단으로 영향을 받거나 거기에 관계될수 있는 비로조단체들을 위하여 로조대표와 접촉하는 방법이 반영되여야 한다. 바라건대 신속한 통보를 하면 로조는 재난에 복잡성을 더해주는것이 아니라 재해복구와 직원조정활동에 도움으로 된다.

회사안에 로조가 있건없건 인사과는 재해복구사업에 개입하여 해당 로동관계법이나 로동관계규정들이 준수되도록 하여야 한다.

위 험 관 리

많은 회사들과 대리기관들은 부서별계획의 조정과 외부 및 내부그룹과의 련락, 위기속에서의 지휘를 총 책임진 위험관리그룹을 가지고 있다. 이 그룹은 회사의 고위관리들과 무제한한 접촉을 가질 필요가 있으며 임의의 업무환경파괴속에서 협조 및 지도에 대한 위임권을 가지고 있어야 한다. 이러한 위임이 없이는 위험관리그룹이 흔히 위기속에서 도움을 줄수 있는 기본문제전문가(SME)들을 얻기 어려울수 있다. 왜냐하면 또 다른 그룹의 관리자가 그들을 자기의 기본의무로부터 떼여 내기를 거절하기때문이다.

위기속에서 이 그룹의 4가지 집중령역은 통보, 협조, 통제, 조정이다. 정확히 설정된 그룹을 가진 회사는 누가 담당자이며 상반되는 명령을 전달하고 있는가를 확신하지 못하는 경쟁그룹들의 《알렉싼더 하이그증후근》을 방지할수 있다.

이 그룹성원들가운데서 한 사람이 필요할 때마다 회사의 건강 및 안전그룹의 성원으로 되여야 한다. 이러한 위기속에서 개별적로동자들의 건강문제 즉 정신적, 물리적건강에 정확한 주의가 돌려 지도록 하여야 한다.

재난속에서 위험관리그룹은 또한 회사 또는 재난에 관계되는 모든 광고활동을 정지 혹은 금지시키며 개인들이나 기관이 대중보도를 주시하도록 하며 회사의 성명과 발표가 어떻게 사회에 접수되고 있는가에 대한 반향을 회사에 알려 주도록 하여야 한다.

많은 위험관리그룹에서 놓칠수 있는 두개의 인자는 재해복구기간 비상사태운영쎈터(EOC)와 고장싸이트의 관리유지와 보안이다. EOC에 대한 접근을 제한하고 그것을 깨끗하고 어지럽지 않게 유지하는것은 쎈터의 원활한 운영에 도움이 될것이다.

EOC는 회복운영에 포함된 직원들의 가정과 접근회선을 가지고 있어서 그들이 통보를 전달하거나 새로운것을 수신할수 있도록 해야 한다. 가정적문제를 리해하고 해결하는 것은 개인들이 회복노력에 집중할수 있게 하는데서 중요한 문제이다. 추가로 회사는 위기와 직접적으로 련관되지 않은 다른 종업원들에 대한 새로운 자료를 제공하는 자동전화대답기계와 전화회선을 가지고 있어야 한다. 이것은 또한 작업싸이트와 보고정보를 종업원들에게 중계하는데 리용될수 있다.

재해복구운영은 흔히 지역관리자의 정상한계를 초과하는 자금지출을 동반한다. 승인과정을 가속시키고 일시적으로 소비한계 증가를 승인하는 지령사슬이 개발되여야 한다. 또한 위기로 영향을 받은 가정들이나 개인들에게 보장될 선불금에 대한 지불장부처리가

필요하다.

위험관리그룹은 회사의 주요고객목록을 가지고 회사가 운영중에 있다는것과 개정된 접촉방법을 알려 주어 전화문의가 즉시 이루어 질수 있도록 해야 한다. 이것은 고객들에 의한 계약손실 또는 손상된 신뢰를 방지할수 있게 한다.

정 리 해 고

정리해고는 정보체계보안에 지금까지 막대한 영향을 주었다. 그것은 많은 직능을 통합하여 직무상구별을 없앴으며 많은 사람들이 정확한 훈련이나 경험이 없는 과제들을 맡게 한다. 이 경우에 부적당한 문서화가 회사에 손해를 끼칠수 있다. 흔히 작은 일자리들이 없어 지면 직원은 해고된다. 보조부문사람들은 특히 정리해고대상으로 되기 쉽다. 그것은 그들이 하는 사업의 리익과 중요성이 잘 인식되지 않기때문이다.

정리해고는 또한 회사에 대한 근로정신과 성실성에도 영향을 미친다. 정리해고제안이 회사에 4주에 해당한 생산량의 손해를 준다는 사실이 평가되였다. 이때 정보체계보안전문가들은 보안에 위험을 주거나 가능한 불만행위에 대하여 더 큰 주의를 돌려야 한다.

다른 조사자료에 의하면 보통때 종업원들중에서 10%가 회사에 대하여 사취할 기회를 가지고 있는것으로 되여 있다. 정리해고기간에는 이것이 약 30% 정도로 늘어 날수 있다고 한다.

문 서 화

문서화는 앞에서 론의하였지만 여기서 한번 더 설명할 필요가 있다. 어떤 고장후에 또는 업무재개계획검사 및 재해복구노력 이후에는 즉시에 모든 문서화를 재검토하여 문서화의 모든 개선과 변경을 기록해야 한다. 문서화의 최후변경만 리용가능할수 있도록 해야 한다(이것은 문서들에 번호를 붙임으로써 달성될수 있다).

부분적처리: 누가 우선권을 가지는가

재난기간에는 모든 부서들이 우선권봉사를 요구한다. 그러나 그것을 판단하고 다중과제처리를 조작할 여유가 없다. 업무재개 및 재해복구계획을 개발하는데서 필수적인것은 회사의 어느 부분에 첫째가는 주목을 돌려야 하는가를 결정하는것이다. 많은 계획들에서 계획은 모든 업무과정들을 회복할수 있는 하드웨어 또는 처리능력을 포함하지 못한다. 정확한것들이 회복되도록 해야 한다. 계획이 일단 개발되면 모든 관리자들은 서명을 하여 그들이 사고시에 누가 첫 우선권을 가질것인가를 인식하고 접수하도록 해야 한다.

주의해야 할 기타 재난

위험관리그룹과 모든 업무재개계획작성자들의 일상적인 과제는 회사의 업무과정이나 재해복구계획에 영향을 줄수 있는 사건진행과정을 감시하는것이다. 실례로 회사는 린접시설에서의 사고나 자기의 운영능력에 영향을 미치는 환경상위험에 대해서도 무심히 대하지 말아야 한다. 그러자면 재해복구계획에 영향을 미칠수 있는 재난진행과정에 대하여 알고 있어야 한다. 이러한 한가지 실례는 세계무역쎈터에 대한 폭격사건이다. 몇주일후에 구조물고장(폭설로 지붕까지 묻혀 버림)으로 인하여 자료쎈터를 잃어 버린 한 회사는 계약된 강력한 싸이트로 옮겨 갈수 없었다. 왜냐하면 그것은 이미 세계무역쎈터에서 온 다른 회사들이 리용하고 있었기때문이다. 만일 그 회사가 이에 대하여 주의를 돌리고 있었다면 이것이 자기의 재해복구계획에 영향을 미칠것이라는것을 알았을수 있으며 고장에 대처하여 다른 싸이트를 지정하는 조치를 취했을수 있다.

재해복구계획은 장기간에 대처할 필요가 있을수도 있다. 실례로 최근에 있은 강한 폭풍으로 하여 일부 회사들의 공업전원이 몇주동안 차단된것을 들수 있다. 초기에는 업무운영을 다시 시작할수 있었지만 그들이 며칠동안의 예비전원만을 계획하였기때문에 그것을 계속 유지할수 없었다.

요 약

정보체계보안전문가들은 업무재개계획화와 재해복구분야에서 관건적인 역할을 수행한다. 이것은 대부분의 정보체계보안일군들의 정상의무에서 급격히 리탈하는것이다. 그들은 엄밀한 기술적 또는 체계적리해보다는 전체 업무과정에 대한 리해와 재난환경속에서 어떻게 그 과정들을 지원하고 가능하게 할수 있는가에 대한 리해를 가질 필요가 있다. 정보체계보안전문가들이 제공하는 학술적이며 전문가적인 충고는 또한 많은 기관, 회사, 대리기관들이 자기들의 업무과정을 침해하고 급변하는 경쟁시장에서의 생존을 위협할수 있는 사건들에 대처할수 있는 능력을 실질적으로 높여 줄것이다.

참 고 문 헌

1. Quantum Corporation, Disaster Readiness of BCP Professionals, *Disaster Recovery Journal*, Volume 13, Issue 1.

제9편
법, 조사 및 륜리

이 편에서는 콤퓨터사고조사와 전자우편과 인터네트의 리용에 대한 합법적리용측면에서 제기되는 몇가지 문제에 대하여 고찰한다.

제40장에서는 기관망과 정보체계와 관련한 범죄사건을 취급하는 불쾌한 문제를 론한다. 기관이 범죄자를 기소하는 능력을 약화시킬수 있는 그러한 오유를 피하는것은 매우 중요하다. 이 장에서는 상세한 콤퓨터법률분석과 증거사슬고리를 보호하는 보다 빠르고 효과적인 분석방법을 언급한다. 제안한 단계에 따르면 실지로 무엇이 일어 났는가를 결정할수 있는 가능성이 커진다.

제41장과 제42장은 오늘날 기관들이 당하고 있는 현존문제들을 서술한 최근의 사건들을 고찰한다. 첫번째는 인터네트에서 잘 알려 진 불평싸이트에 대한것이다. 이 싸이트들은 목표로 삼은 기관들을 곤경에 빠뜨리는데 그것은 그들이 고객, 종업원, 경쟁자, 판매업체들에 기관에 대하여 불만을 가지게 하기때문이다. 밸리 대 페이버사건을 실례로 든다. 여기에는 페이버가 밸리의 상표를 도용한 사실이 포함되여 있다. 결론은 기관들이 이 싸이트들을 평가하고 거기서 배워야 한다는것이다. 이것은 보편적인 골치거리들이 증가한다는것을 의미한다.

제42장에서는 비요청전자우편다량배포 즉 스팸문제를 어떻게 취급하는가에 대하여 론한다. 실례로는 워싱톤주와 헤켈사이의 소송사건을 들었다. 우의 실례에서 중심문제가 언론의 자유문제인것처럼 이 소송건의 기저에는 워싱톤주의 스팸방지법이 놓여 있다. 여기서는 많은 문제들이 취급되였으므로 이것들을 잘 알아야 앞으로 소송사건에 걸려 들지 않을수 있다. 스팸현상은 우리가 전자우편을 쓰는데서 일정한 장애가 있을수 있으나 이것을 통제하는 방법은 아직 해결되여 있지 않으며 법정에서 더 론의해야 할것이다.

제４０장. 무슨 사건인가

켈리 제이 쿠츠타

밤중에 시체와 범죄현장의 참상과 맞다들렸다고 상상해 보라. 사람들의 극도의 무질서와 혼란상태, 어둡고 침침한 장소에서 연기가 자욱하고 어두운곳에 잔해가 가득 널려있다. 피해자들은 얼이 나가서 왔다갔다 하면서 서로 부딛치기도 한다. 구경하는 사람들과 호기심 많은 사람들이 주변에서 서로 억측도 하고 예측도 하느라고 싱갱이질을 한다. 무슨 일이 일어 났는지 또 언제 일어 났는지 아는 사람은 아무도 없다. 다만 일이 일어났다는것만 안다. 경찰들이 짐작컨대 오고 있는중인것 같다. 그런데 갑자기 누군가가 나에게 달려 오더니 나를 죄인으로 모는것이였다. 왜냐하면 내가 이 동네를 잘 알고 있기때문이였다. 이것은 예상외의 일이며 특히 그 범죄현장이 나의 망가까이에 있거나 나의 정보체계와 관련되는 경우 더욱 그렇다.

이렇게 범죄현장을 비교하여 이야기하는것은 정보체계와 관련된 법적해석문제들이 범죄현장과 류사하기때문이다. 수십년동안 텔레비죤에서 경찰사건문제를 보아 왔기때문에 사람들은 당신이 증거를 인정하지 않을것이라고 생각한다. 왜냐하면 범죄와 관련한 귀중한 정보들과 단서들이 본의아니게 파괴되거나 손상될수 있기때문이다. 범죄현장에서 우리는 의료상방조를 필요로 하는 사람이 없는가를 알아 보아야 하며 그 다음에 전화를 걸어 범죄담당전문가들이 현장에 와서 사업에 착수하도록 해야 한다.

당신의 망에서 불상사가 일어 나고 사건이 일어 났다는것을 늦게야 발견하고 과거의 어느한 일에 대한 정보를 알 필요가 있다면 어떻게 하겠는가. 당신의 기관에 해당한 능력이 있는 사람이 있다면 그 사람에게 그것에 대하여 빨리 알려 주며 또 그 범죄현장을 그대로 보존할것을 바랄것이다.

비상사태대응전문가들이 흔히 말하듯이 사고가 일어 난 직후에 내린 초기결심은 사건수사결과에 가장 큰 영향을 미친다. 오늘날의 정보체계에서는 대체로 징조가 나쁘다는 외부적인 징후들은 외적으로 많이 나타나지 않는다. 사고에 대해서 가장 깊이 아는 사람들은 그 체계사용자들이다.

비밀자료들을 절취하는 현상, 콤퓨터를 다른데 악용하는 현상들은 더 자주 나타난다. 앞으로 사건처리를 사람들이나 회사들이 어떻게 해야 하는가에 대한 최선의 조언을 준다면 그것은 세밀히 관찰할 필요가 있는 해당인원들의 보안관련움직임에 대한 《행동방식모형》을 작성하는것이다(표 40－1). 의심되는 경우 피해자의 콤퓨터에서 하드구동기를 떼서 증거로 보존해야 할 필요도 있다. 하드구동기는 비싸지 않고 그것을 떼고 대신 새것으로 설치하는데 드는 가동중지시간은 얼마 되지 않는다. 이렇게 하면 기관의 자금과 골치거리를 덜수 있다.

기업의 기밀부서에서 사직한 사원을 생각해 보자. 그 사원이 비법적이거나 비륜리적인 어떤 조작을 진행하였다면 사직한 때로부터 30~60일동안까지는 아마 그것을 알아 차리지 못할것이다. 사직하거나 퇴직한 종업원들이 쓰던 탁상형콤퓨터나 무릎형콤퓨터의 하드구동기를 최소 60~90일, 가능하다면 더 오랜 기간 보관하는것이 좋다. 이 기간이 끝

나면 그 디스크들을 깨끗이 청소하여 다시 리용할수 있을것이다. 왜 그런가하면 일단 하드디스크와 그안의 자료가 초기화되여 다른 사람들이 쓰게 되면 그 사건수사에 쓸수 있는 자료들을 수복할 가능성이 거의 없어 지며 투하해야 할 시간과 자금은 모자랄것이기 때문이다.

표 40-1 행동방식모형

종 업 원	위험점수 예 : 1 아니 : 0	무게 100%	무게점수
기밀정보를 다루었는가.	1	5%	0.05
나쁜 마음을 먹고 사직하였는가.	0	20%	0
경쟁자에게 일해 주러 갔댔는가.	1	20%	0.2
미해명사건에 련관될수 있었는가.	0	5%	0
예상치 않게 사직하였는가.	0	10%	0
그의 행동이 소송에 걸려 들수 있는 가능성이 있었는가.	0	25%	0
기관이 비밀정보수집의 대상으로 된적이 있는가.	1	15%	0.15
증거보존점수			40%

증거보존의 지침

0~24% ; 증거를 보존할 필요가 명백치 않다
25~49% ; 증거를 보존할 리유가 충분하다
>49% ; 증거를 보존할 리유가 강하다

대부분의 경우에 증거가 오손된것은 몰라서 그렇게 한것이지 의도적인 기만행위에 의한것은 아니다. 나는 사건이 일어난후에 자기들의 조사솜씨를 발휘하려고 하는 회사나 개인들이 체계관리자들로 하여금 실마리나 흔적을 찾게 하는것을 목격하였다. 어떤 한 사건에서 그들은 증거자료를 발견할수 있었는데 정보를 발견한후 그들은 그 파일을 열고 그것을 플로피디스크에 보관하였다. 이 행위는 기본열쇠로 되는 날자를 변경하고 전자증거를 손상시켰으며 결국 법정에서 리용할수 없게 하였다.

콤퓨터법정전문가들은 체계날자를 관건적인 정보로 본다. 창조, 마지막쓰기 , 마지막접근날자는 과거에 무엇이 일어 났는가에 대한 중요한 견해를 주는 사건순차를 확립하는데 리용된다. 콤퓨터법정학문에서는 콤퓨터법전문가들이 날자를 비롯한 임의의 증거들을 변경시키지 말아야 한다고 지적하고 있다. 의심스러운 체계의 자료를 조사할 때 조작체계가 하드구동기에 자료를 쓰지 않도록 최선을 다해야 한다. 비록 당신이 콤퓨터법전문가가 아니라고 해도 당신은 원래의 증거를 보존함으로써 자기 회사가 범죄에 대처할수 있도록 해야 한다.

콤퓨터가 기동할 때 조작체계는 즉시 체계의 많은 파일날자를 변경하거나 수정한다. 실지 그 파일개수는 기관이 어떤 체계, 항비루스응용프로그람, 망규약을 리용하고 있는가

에 관계된다. 표준적인 Windows 98 체계들은 12,000개이상의 파일을 관리한다. 기동과정에 수백개의 파일들이 POST(Power On Self Test)기간에 변화될수 있다.

항비루스응용프로그람이 설치된 경우에는 악성코드를 제거하는것이 곧 그 파일을 변경시키는것으로 된다. 이 과정은 마지막접근 및 마지막쓰기날자를 변화시킨다.

가능한껏 많은 선택을 리용할수 있게 하기 위하여 적당한 시간동안 하드구동기를 떼여 놓아야 한다고 생각된다. 만약 당신이 매 하드구동기를 검사상태로 놓는것을 잠재적인 비용때문에 할수 없다면 그것을 제한된 기준하에서 실행할수 있다고 생각된다. 이미 나는 하드구동기를 보관해야 할 필요가 있는 퇴직사원에 대한 행동방식모형을 개발할것을 언급하였다. 그 목적은 앞으로 콤퓨터의 하드구동기를 조사할 필요를 지적하는 예측수단을 얻자는것이다.

나의 경험은 인간의 행동이 수자식범죄현장에서 고려되여야 할 중요한 예측수단이라는것을 보여 준다. 매개 기관은 사실상 경고와 같은 각이한 행위들을 체험한다. 매개 기관들은 그 수준에 맞는 자체의 행동방식을 개발할 필요가 있다. 이 경우에 과거의 사건은 미래의 사건에 대한 가장 좋은 지시자이다. 고려해야 할 정보원천은 합법적인 기관이나 업무단위 그자체는 물론 인적자원, 공동조사, 정보보안이다.

당신의 행동방식모형에 고려해야 할 요인들은 다음과 같다. 그 사원이 기밀자료를 다루었는가, 사직이 뜻밖이였는가, 퇴직이 법적소송을 일으킬것 같은가, 사원이 경쟁자를 위해 일하려 하지 않는가, 사원이 접촉한 기관과 관련한 어떤 사건이 없었는가, 그가 왜 떠나려고 하는지 애매한 점은 없는가. 우의 임의의 물음에 대해 《예》라는 대답은 최소한 적당한 기간 하드구동기를 보존할 필요성을 제기할것이다.

나는 사원 혹은 이전의 사원문제를 취급할 때 《나는 그 사람에 대하여 의심스러운 점이 있다는것을 알았다!》라는 말을 자주 듣는다. 이밖에도 경시한 다른 문제들이 있는데 모든 요인을 고려해 보면 기관들이 경고징후들을 놓쳤다는것을 돌이켜 보게 된다. 경고들은 일반적으로 인적자원, 공동조사, 업무단위, 정보보안을 비롯하여 여러 령역에 퍼져 있다.

인적자원과 업무단위는 개인의 행동이나 사원이 떠나려고 하는 가능한 원인에 대한 열쇠를 가지고 있다. 공동조사는 외부사건이나 지적정보에 대한 견해를 줄수 있다. 이것은 알려 지지 않았지만 조사중에 있는 사건, 사적경영정보를 얻기 위한 적수의 기도 그리고 다른 가능한 관련문제를 포함한다. 정보보안은 개인들이 최근에 표현한 의심스러운 행위에 대한 어떤 정보를 가질수 있다. 의심스러운 행위의 실례로서는 기밀자료에 대한 접근기도, 방대한 자료의 복사, 기술오용의 변명, 의심스러운 인터네트싸이트에 대한 열람 등이다.

내가 목격한 가장 좋은 방법은 사원퇴직과정을 맡은 인사과직원들이 우에서 말한 세개의 그룹에 통보하게 하는것이다. 그들은 매 그룹에 적당한 시간을 주어 금지된 기간 하드구동기를 보존하거나 구체적인 사건과 관련되는 즉시적인 분석을 요구할수 있다. 물론 인사과직원은 자기들의 정보에 기초하여 직접 요청할수 있다.

신입직원들을 가르치는데서 《허용되는 사용》방책이 가지는 중요성을 잊지 말아야 한다. 퇴직하는 사원들이 자기들의 콤퓨터를 반환하려고 할 때 그들에게 무엇을 할수 있고 무엇을 할수 없는가를 지시해야 한다. 업무요구와 수준에 따라 당신은 사원들의 밀기

(wipe)편의프로그람(특히 비표준제품) 혹은 법정결과를 방해할수 있는 다른 제품들의 사용가능성을 제한하는 방책을 확립할수 있다. 비록 이것이 기업들에서 론의하기 어려운 문제라 하더라도 이것은 매우 사활적이다. 나는 약간의 불만을 품은 사원이 고의적으로 유용한 의뢰기정보를 지우고 편의프로그람을 써서 그 정보를 회복할수 없게 만든 사건을 여러번 보았다. 설사 이 문제에 대한 방책이 없다고 하더라도 당신은 리성적인 판단을 내려야 한다.

당신의 기관에 알맞는 방법을 개발하기 위해서는 우에서 지명한 개별적사람들과 당신의 변호사로부터 정보를 얻어야 한다. 만약 그 사원이 로조성원이라면 특수한 규정을 적용할수 있다. 또한 주의 법에 기초한 혹은 기관이 정부와의 계약을 리행하는가에 대한 특수한 고려가 있을수 있다. 보존된 증거는 아마도 호출장과 함께 제출될 것이다. 당신의 변호사는 당신이 어떤 법적요구를 주장해야 하는가를 결심하도록 할 것이다.

우에서 말한것과 비슷한 방법을 받아 들인다고 가정하자. 기관은 하드구동기를 보존하기로 결심하였다. 당신은 그에 대해 어떻게 하려는가. 기본관심사는 련속적인 보관을 확립하고 특수한 세부내용을 문서화하고 하드구동기를 안전하게 유지하는것이다. 만약 당신이 보존한 전자증거가 법정에 제출될 기회가 있다면 이 모든것은 극히 중요하다.

당신은 련속적인 보관을 확립하여 인증을 확인하고 증거위조라는 주장을 반박해야 한다. 만약 당신이 그 증거가 당신의 관리하에 있었다는것을 증명할수 없다면 당신은 유죄증거를 위하여 변경되거나 수정되지 않았다는것을 증명할수 없다고 많은 변호사들은 공격할것이다. 련속보관을 확립하기 위하여 당신은 문제가 해결될 때까지 수집한 순간부터 입수물을 문서화해야 한다. 여기에는 법정체계를 통한 상소과정이 포함된다.

문서화과정의 일부로서 증거가 발생한 본래의 PC에 대하여 가능한껏 많은 세부내용을 식별하여야 한다. 이것은 중요하다. 왜냐하면 몇개의 관건적인 정보가 알려 지는 경우 후에 완성된 분석이 훨씬 원활하게 될것이기때문이다. 다음과 같은 문제들이 문서화되여야 한다.

- 하드구동기에 어떤 조작체계가 있는가.
- 기타 체계명세는 무엇인가(RAM, SCSI, IDE; 처리기형태).
- 구동기분할(Partition)이 어떻게 되여 있는가.
- 하드구동기에 어떤 응용프로그람이 있는것으로 알고 있는가.
- 어떤 암호화가 리용되는가.
- 알려 진 통과암호, 열쇠, 인증서목록이 있는가.
- 하드구동기의 소유자는 어떤 체계에 접근하고 있는가.
- 하드구동기는 어떤 형태의 체계에서 만든것인가(제작업체, 모형).
- 보수경과기록을 비롯한 하드웨어문제들에 대한 기록이 있는가.

이 질문들에 대답을 주면 법정분석이 훨씬 빨라 지고 효과적인 과정으로 될것이다.

1차경과기록은 그것이 수집된 때로부터의 증거를 동반해야 한다. 그것은 날자와 시간, 상세한 증거자료서술, 누가 증거를 포착하였는가 등을 포함해야 한다. 경과기록은 또한 보관부서에 전송되여야 하며 거기에는 전송리유와 방법(인편전달), 발송자와 날자(전송자의 서명과 날자), 접수자와 날자(접수자의 서명과 날자)가 포함되여야 한다. 증거를 보관하고 있는 사람들은 그 증거가 자기들의 수중에서 안전하게 보호된다는것을 증명할 필요가 있다.

안전한 장소는 접근이 제한되는 페쇄가능한 용기이다. 그것은 자물쇠가 있는 파일보관장, 금고, 증거보관함, 지어는 쇠를 잠그는 방일수 있다. 가장 좋기는 그 증거에 꼭 한 사람만이 접근하게 하는것이다. 그것이 불가능하다면 증거를 제한된 구역에 기억시키고 그 구역에 접근하는 사람을 다 문서화하여야 한다. 증거에 보다 많은 사람이 접근할수록 그것은 보다 많은 사람이 증거를 변경시키지 않았음을 증명해야 한다는것을 의미한다. 단일접근을 허용하는 페쇄용기를 준비하는것은 다중접근용기보다 더 쉽다. 만일 증거를 규칙적으로 안전하게 보존하려 한다면 증거보관함을 구입하여야 한다. 증거보관함은 보관하고 있는 증거에 대한 1차경과기록도 포함해야 한다. 증거가 보관되면 그것은 등록되여야 한다. 증거가 제거될 때마다 보관은 개인들에게 전송되여 제거되여야 한다. 우에서 보여 준 경과기록들에 대한 설계를 여기서 리용할수 있다. 이 경과기록의 목적은 증거보관함이 접촉될 때마다 매번 문서화하는것이며 특정한 증거에 대한 문서화를 지원하는것이다.

증거를 다른 곳으로 보낼 필요가 있다면 그 보관에 대한 문서화를 보장할수 있는 려행안내자봉사를 리용하는것이 좋다. 여기에는 형식과 개수를 추적하는것도 포함되여야 한다. 전통적인 송달봉사의 대부분은 이 봉사를 제공한다. 송신자들은 짐함을 밀봉해야 하며 수신자들은 그것이 터지지 않았는가를 관찰해야 한다. 추가적인 보호로서 증거를 용기안에 밀페하여 수신자가 그 문서가 위조되지 않았음을 증명할수 있도록 해주는것이 필요하다. 전송도중에 증거를 보호하기 위한 합리적인 조치들을 취해야 한다. 증거가 손상된다면 그것은 거의 쓸모 없게 된다.

이런 단계들을 거치면 지난 기간에 무엇이 일어 났는가를 결정하기가 쉬워 질것이다. 력사가 미래를 변화시키리라는것을 리해하는것이 최종적인 목적이다. 력사를 리해하기 위하여 우리는 훌륭한 정보를 가지고 있어야 한다. 정보를 보존하기 위하여서는 콤퓨터법률전문가로 될 필요까지는 없고 다만 그 과정을 리해하고 왜 그것이 중요한가를 리해하면 된다. 또한 회사가 효률적인것으로 되게 하며 《무엇이 일어 났는가》에 대한 좋은 정보를 가질수 있도록 실천기술에 숙련하여야 한다.

제４１장. 인터네트불평싸이트와 밸리 대 페이버사건

에드워드 에이취 프리맨

어느 큰 기관들에나 다 불만을 품은 사원들과 의견 있는 고객들이 있다. 최근까지만 하여도 불만 있는 사람들은 자기의 불평을 흔히 친구들이나 동정하는 사람들에게 털어놓는것이 고작이였다. 기관들에서는 그 불평을 공개적으로 거부하면 오히려 그 불평에 사회적으로 더 관심이 집중될가봐 무시하는 경우가 많았다.

인터네트의 폭발적인 증가로 하여 의견 있는 고객들이 기관들을 비판하기가 더 쉬워졌고 그들의 신소를 더 많은 사람들이 쉽게 듣고 볼수도 있게 되였다. 《불평싸이트》는 인터네트에서 평범한것으로 되였다. 거의 모든 큰 기관들과 보다 작은 많은 기관들이 이 불평싸이트의 대상이 되였다. 이런 싸이트들에는 싸이트운영자의 불만뿐아니라 의견 있는 고객들, 사원들, 경쟁자들 지어 판매업자들도 그 기관에 대한 고소장을 게시하는 정도이다. 기밀적인 내부문건들도 이러한 Web페지들에 나오고 있다. 어느 회사의 고객으로 되려는 사람들과 직업을 얻으려는 사람들은 그 회사와의 거래건이나 제공하는 직업을 받아 들이기전에 꼭 이 싸이트들을 방문하고서야 결심을 채택하군 한다. 이런 싸이트들은 매달 수천건의 대인기글들을 받군 한다.

비록 작지만 이 불평싸이트들은 큰 회사들 지어 누구도 어쩌지 못한다는 대규모회사들에도 큰 골치거리로 될수 있다. 인터네트의 공개적성격에 의하여 콤퓨터 한대와 불평할것만 있으면 100딸라미만으로 나쁜 이름을 가진 Web싸이트를 하나 구매할수 있다. 싸이트들에 게재되는 신소장들은 추적이 불가능하게 되여 있으므로 그것이 진실인지 아닌지를 확인해 볼수 없게 되여 있다.

이 장에서는 밸리 대 페이버라는 불평싸이트들을 둘러 싼 1998년 련방재판소 판결을 보기로 한다. Bally Total Fitness라고 하는 전국적인 망의 운동구락부는 자기의 등록상표명을 부정적으로 사용하고 있는 어느 한 인터네트싸이트를 닫아 치우려고 시도하였다. 여기서는 주로 상표사용권위반문제와 상표희석화문제를 보기로 하자. 이 글 전반에서는 실지 법정사건들을 실례로 리용하였다.

밸리 대 페이버사건의 진상

Bally Total Fitness(그림 41－1 참고)는 쉬카고우에 국제적인 본부를 두고 있는 뉴욕주식시장의 한 회사이다. 밸리회사는 국내에 27개주와 카나다에 360개소의 시설을 둔 근 4백만의 성원들을 망라하고 있는 북아메리카에서 가장 큰 영리기관으로서 건강체육구락부들을 운영하고 있다.

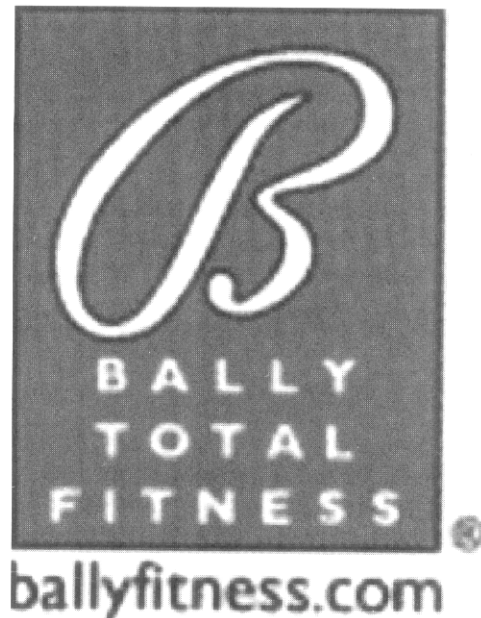



그림 41－1. 밸리의 마크

워싱톤시에 사는 사진업자이며 Web설계가인 앤드루 페이버와 밸리회사사이에 분쟁이 있었다. 분쟁문제를 자기에게 유리하게 해결하지 못한 그는 《Bally Sucks》(밸리는 이렇게 빨아 먹는다)라는 Web싸이트를 개설하고 운영하였다. 그 싸이트는 밸리에 대한 소비자들의 불평을 담는 전용싸이트로서 그들이 밸리건강체육구락부 성원이기를 그만두려면 어떻게 해야 하는가에 대한 사항까지 알려 주었다. 페이버의 싸이트는 밸리회사가 아닌 다른 회사에 대한 불만을 가진 고객들도 자기들의 이야기를 하도록 적극 장려하였다. 그러던중 어떤 Web써퍼(surfer)가 그 싸이트를 방문했는데 거기에는 밸리의 뚜렷한 상표(그림 41－1)가 나타나고 그우에 두드러지게 sucks(빨아 먹다)라는 글이 나타나는것이였다. 스크린의 밑부분에는 《Bally Total Fitness Complaints! Un–authorised》(밸리건강체육구락부불평마당) (Un–authorised는 《허가를 받지 않은》이라는 뜻도 있으나 《저자가 없는》이라는 뜻도 나온다–역주)라는 글도 있는것이였다.

1998년 2월 밸리회사는 캘리포니아주의 련방재판소에 페이버를 기소하였다. 밸리는 자기의 상표를 페이버가 사용중지할것을 요구하였다. 밸리는 페이버의 Web싸이트가 상표권침해, 부정경쟁, 상표희석화를 방지하는 법률을 위반하고 있다고 주장하였다. 4월에 법정은 페이버에 대한 림시억제명령을 밸리가 신청한데 대하여 기각하였다.

11월에 법정은 밸리에 대한 략식판결을 할데 대한 페이버의 신청을 승낙하였다. 략식판결은 《물질적사실에 관한 진정한 소재가 없으며… 신청자측이 법률상 재판할 권리가 있는》경우 재판소들에서 리용하는 수법이다. 략식판결신청제기를 승인함으로써 법정은 밸리의 주장이 모두 사실인 경우라 하더라도 그 사실들만 가지고는 밸리의 소송사건을 증명할수 없다고 주장하였다. 밸리는 평결을 하소하였으나 련방재판소의 판결이 나오기전에 쌍방이 문제해결을 타결 지어 페이버가 《밸리는 빨아 먹는다》라는 자기의 Web싸이트를 철회하였다.

상 표 법 개 관

상표란 판매자가 자기의 제품에 붙여 그 생산지를 식별하여 그 상품을 다른 상품들과 구별하는 뚜렷한 그림이나 단어이다. 상표법은 다음의것을 포함한 많은 식별형태들을 보호한다.

- Kodak나 Exxon과 같은 고안된 단어들
- Heinz Ketchup 유리병과 같은 뚜렷하며 고유한 포장용기
- 독특한 색배합(Kodak 필림의 노란색과 붉은색의 배합)
- 건축도안(McDonald간이식당의 황금아치형앞문)
- 고유한 로고(logo)와 상징물(IBM의 상징이나 Kellogg사의 붉은 K자)

1946년 국회는 상표를 규제하기 위하여 《란함법(Lanham Act)》을 통과시켰다. 주들사이의 호상 상업무역을 규제할데 대한 헌법적권리밑에 국회는 이 법을 발효시켰다. 이 법에 준하여 등록된 상표는 련방보호를 받는다. 당사자들은 완성상표나 상표계획안을 특허 및 상표국에 등록할수 있으며 국에서는 이것을 검열관들이 초기비준하면 특허 및 상표국국지에 공개한다. 이 목적은 다른 대방들로 하여금 최종비준을 예비적으로 통지하게 하는것이다. 상표분쟁문제를 해결하기 위해서는 많은 법적선택사항들이 제기된다.

이 법은 또한 상표로 법적등록을 할수 없는 일련의 마크에 대해서도 언급하고 있다. 그것들은 다음과 같다.

- 통칭적이거나 지명이 붙은 상품의 이름(실례로 Maine Potatoes는 그 어느 개인의 상품명으로 등록될수 없다. 이 단어들은 그 어느 개인제품을 가리키는것이 아니라 메인주에서 생산되는 감자전체를 가리킨다. 그러므로 Johnson's Maine Potatoes라고 하면 상표로 등록할수 있다).
- 본인의 승인이 없는 산사람의 이름, 초상, 서명
- 주 또는 시의 기발

상표의 소유주는 그 상표에 대한 《전용권》을 담보 받기는 하지만 그 전용권에도 일정한 제한이 있다. 그 제한성을 《공정한 사용권》이라고도 하는데 이것은 다른 사람들이 그 제품을 묘사하기 위하여 그 상표를 쓸수 있다는것을 의미한다. 바로 그 공정사용권이 있음으로 하여 밸리의 상표가 이 장에서 설명을 위해 제시될수 있는것이다. 만일 1985년도산 쉐브롤레이 쎌리브리티형승용차를 팔겠다면 제네럴 모터스회사에서 그 상표사용허가를 받지 않았어도 이 자동차는 쉐브롤레이 쎌리브리티라고 광고할수 있다. 경쟁자들도 상품비교에서 남의 기록상표를 리용할수 있다. 실례로 코카콜라광고에서는 비록 펩시콜라회사에서 자기 상표를 사용할 권한을 주지 않았어도 펩시콜라보다 맛이 더 좋다고 광고할수 있다.

사람들과 기관들은 상품구매에서 많은 경우 상표에 기초하여 옳바른 결심을 한

다. 이 법에 의하면 상표권침해로 인정할수 있는 경우는 타방에 의한 상표사용이 《혼란을 일으키거나 실수를 초래케 하거나 기만을 목적으로 할수 있는 경우》이다. 법정은 이런 경우 금지명령을 내리거나 손해배상을 시키거나 침해자의 리윤을 몰수하거나 변호비를 물릴수 있다. 법정은 지어 비법상표를 가진 제품들을 몰수하여 페기할수도 있다.

상표소유주는 자기 상품을 자기 제품뿐아니라 그 관련제품 례하면 티샤쯔나 점심밥곽 등에도 사용할수 있는 독점적사용권을 가진다. 권위 있는 인정된 상표는 해당 회사의 가장 귀중한 재산일뿐아니라 회사를 팔거나 청산할 때에는 화페적가치를 가진다.

상표희석으로 인정되는 경우는 상표의 비법적사용이 상표의 소유주에게 있어서 재정적손해를 주는 경우이다. 상표희석은 반드시 상업적성격을 띠여야 가능하며 대방들사이의 직접적인 상업적경쟁이 없는 경우에도 발생할수 있다. 최근의 한 실례에서 볼수 있는 바와 같이 세계적인 신용카드업체인 American Express는 American Express Limousine Service회사가 자기의 이름을 사용하자 이 회사를 소송에 제기하였다. 두 회사사이에 경쟁적인 측면은 없었음에도 불구하고(하나는 신용카드회사이고 다른 하나는 승용차봉사회사이므로) 법정은 《피고측이 American Express라는 마크를 사용한데 대하여 이것은 원고의 마크의 뚜렷한 질에 손상 줄수 있다》고 판결하였다.

상표권침해에 대한 분석

밸리회사는 페이버의 Web싸이트가 상표권침해는 물론 상표희석에도 해당되는 범죄로 된다고 주장하였다. 략식판결에서 법정은 밸리측의 모든 기소내용이 진실이라고 해도 페이버측의 행동은 상표법위반으로 되지 않는다고 판결하였다. 상표법에 따르면 법정은 밸리측의 상표를 페이버측이 사용한것은 혼돈의 가능성이 있다고 판결하여야 했었다. 그렇게 되는 경우에만 법정은 상표권침해가 일어 났다고 볼수 있었다.

혼란가능성이 있는가 없는가를 결정하는데서 기본요인은 두 대방의 제품에서의 류사성이다. 제품들의 호상관계가 더 뚜렷할수록 법정이 상표권침해를 인정할수 있는 가능성은 더욱 커진다. 《관련 있는 제품이란 비록 꼭 같지는 않아도 소비자들이 관련되는 제품이라고 보는 그러한 제품들이다.》 법정들에서는 지금까지 다음과 같은 쌍의 제품부류들을 관련상품으로 보아 왔다.

- 샤쯔와 바지
- 맥주와 위스키
- 자물쇠와 손전지

밸리측과 페이버측은 상품들을(하나는 건강구락부이고 다른 하나는 Web페지설계이므로) 판매하지 않았기때문에 관련상품을 통한 혼란의 우려는 거의 없었다. 그리하여 법정은 다음과 같이 판결을 내렸다.

밸리측의 공식적인 Web싸이트와 페이버측의 싸이트를 비교해 보는 그 어느 리성적인 소비자도 페이버측의 싸이트가 해당 상표소유자의 상표와 같거나 련관이 있다거나 소속이 같다거나 후원을 받는다고 생각하지 않을것이다. 따라서 상표권침해에 관한 밸리측의 상소는 법적으로 성립되지 않는다.

상표희석에 대한 분석

법정은 또한 상표희석이라는 밸리측의 주장을 략식판결할데 대한 페이버측의 신청을 허락하였다. 상표가 희석되였다는것을 증명하려면 피고의 상표사용에 의하여 원고의 상표가 자기 상품 및 봉사를 구별하고 식별하는 능력이 떨어 져야 하며 피고의 상표사용이 상업적성격을 띠여야 하는것이다. 상표희석이라는 주장을 증명하자면 밸리측이 페이버가 자기 상표를 상업적목적에 리용하였다는것을 보여 주어야 하였다. 또한 밸리측은 페이버에 의한 상표리용으로 하여 자기 회사제품 및 봉사를 구별 및 식별하는 자기 마크의 능력이 떨어 져 상표의 가치가 희석되였다는것을 보여 주어야 하였다.

사실 페이버가 밸리측 상표를 리용한것은 비상업적인 성격의것이였다. 그는 그 상표를 리용하여 자기 기업의 리익을 추구한적도 없으며 따라서 밸리측은 페이버의 상표리용이 그 상표의 명예에 손상을 주었다는것을 제시할수 없었다. 또한 페이버의 싸이트는 소비자들을 혼란시키지는 않았으므로 법정은 략식판결제안을 수락하였던것이다.

기관들에 주는 권고

가장 안정하다고 생각되는 회사일지라도 불평싸이트들은 골치거리가 아닐수 없다. 고객희망자들과 사원신청자들은 꼭 이러한 싸이트를 보고야 마는것이다. www.walmart sucks.com은 지난 3년간 100만건이상의 급소를 찌르는 대인기작품들을 접수하였다고 한다. 이러한 문제점들을 미연에 방지하기 위한 일련의 권고사항들을 아래에 준다.

일부 기관들은 가능한 불평싸이트의 이름들을 실지로 구매함으로써 외부사람들이 불평싸이트를 볼수 없게 한다. 실례로 chase Manhatan은 IhateChase.com, ChaseStinks.com, ChaseSucks.com, ChaseBlows.com 등 이 책에서는 차마 다 말하지 못할 여러가지의 가능한 불평싸이트들에 대한 Web싸이트권을 사들였다. 그렇게 하였음에도 불구하고 어느 한 불평을 품은 고객이 자기의 불평싸이트인 chasebanksucks.com을 설립하였다. 어쨌든 이렇게 해놓으면 고객희망자들이 그 싸이트를 발견하기 더 힘들것이다.

기관들은 정상적으로 자기들과 관련된 불평싸이트들을 읽어 보는것이 현명할것이다. 인터네트의 자유라는 성격으로 하여 어떤 Web싸이트의 내용에 대한 실제적인 통제는 없다. 어느 한 사람이 불평이 있다고 해서 거짓소문을 퍼뜨리면 그것으로 하여 종업원들의 사기가 저락될수 있으며 지어 회사의 명예에 금이 갈수도 있다.

마지막으로 각 기관들은 불평싸이트에 대한 자기들의 관점을 바로 가져야 한다. 대

부분의 불평싸이트들은 한명의 의견 있는 고객이나 이전 종업원이 단지 자기의 울분을 토로하는것으로는 크게 해를 주지 못한다. 대부분의 이런 싸이트들은 그 내용에서 사람들을 위협하는것이 없다든가 내부보안의 약점을 통하여 입수한 현재의 비밀문건들을 게시하지 않는한 무시해 치워도 안전하다.

결 론

벨리 대 페이버사건으로 하여 개인들은 혼돈의 가능성이 없는한 이러한 불평싸이트들에 상표화된 마크를 리용할수 있게 되였다. 인터네트가 더욱 확대됨에 따라 불평싸이트들은 더욱 범상한것으로 될것이다. 각 기관들은 이 싸이트들을 잘 평가하여 봄으로써 자기 고객들과 사원들과의 관계를 어떻게 가져야 하겠는가를 배워야 할것이다.

참 고 문 헌

1. www.ballyfitness.com
2. Andrew Malone, Masters of their domain, the scramble for insulting Web sites, *New York*, June 8, 1998.
3. Fed. R. Civ. P. §56(c).
4. 15 USC §§1051–1127.
5. Article I, Section 8, Clause 3.
6. Mark Warda, *How to Register a United States Trademark*, Sphinx Publishing, Clearwater, Florida, 1988, 10–11.
7. §32[a][1].
8. Steven W. Kopp and Tracey A. Suter, Trademark strategies online: implications for intellectual property protection, *Journal of Public Policy & Marketing*, Spring 2000, 119.
9. J. Thomas McCarthy, *McCarthy on Trademarks and Unfair Competition*, §24:89 at 24-137-38 (1997).
10. *American Express v. American Express Limousine Service*, 772 F. Supp 729 (E.D.N.Y. 1991).
11. 15 USC §1114(1)(a).
12. *Petro Stopping Centers, L.P. v. James River Petroleum, Inc.*, 130 F.3d 88 (4th Cir. 1997).
13. *Levi Strauss & Co. v. Blue Bell, Inc.*, 778 F.2d 1352, 1363 (9th Cir. 1985).
14. Id.
15. *Fleischmann Distilling Corp. v. Maier Brewing Co.*, 314 F.2d 149, 152–53 (9th Cir. 1963).
16. *Yale Electric Co. v. Robertson*, 26 F.2d 972 (2d Cir. 1928).
17. *Bally*, 1163–1164.
18. Note, "Bally Total Fitness Holding Corp. v. Faber," *15 Berkeley Tech. L.J.* 229, 2000.
19. Robert Trigaux, Bank-bashing goes digital at Internet gripe sites, *American Banker*, March 26, 1999, 1.

제42장. 비요청전자우편에 대한 통제

에드워드 에취 프리맨

인테네트사용자들로부터 가장 자주 신소 받는 문제의 하나가 바로 스팸(spam)이라고 부르는 비요청전자우편의 범람이다. 이것을 사면 부자가 된다는 식의 판매선전으로부터 금연토론회, 바이애그라(최음제의 상품명–역주)로부터 탈모증치료법에 이르기까지 이러한 비요청전자우편은 별것을 다 판매하려고 애 쓴다. 인터네트사용자라면 그 누구든 이렇게 끊임없이 들이닥치는 비요청전자우편의 성화를 면할 방도가 없다. 스팸의 세계에서는 그 어떤것을 주장해도 어처구니 없지 않으며 그 어떤것을 약속해도 황홀하지 않게 된다.

다량의 전자우편을 보내자면 간단히 한대의 개인콤퓨터와 모뎀이면 충분하다. 249딸라를 내면 1천 1백만명이상의 전자우편주소를 담은 CD–ROM 한장을 살수 있다. 이렇게 되면 우편료도 인쇄비도 필요 없고 주문이나 고객들의 문의편지를 처리하는 전문인원을 채용할 필요도 없다.

스패머(스팸하는 자)들은 다량전자우편의 비용을 말단사용자들과 인터네트봉사제공자(ISP)들에게 넘겨 씌운다. ISP는 그들대로 비요청전자우편의 처리 및 전송을 위하여 보충적인 대역너비와 보관장치들을 제공해야 하는것이다. 보충적인 보관능력까지 리용하여 전자편지들을 보관하였다가 해당 수신자에게 넘겨 주어야 한다. 이 비용이 결국에는 다 전자우편사용자에게 부과된다.

이 장은 워싱톤주가 스팸에 대한 엄격한 법률을 실시하기 위하여 어떻게 시도하고 있는가를 취급한다. 여기서는 국가헌법의 통상조항과 함께 개별적주들이 서로 다른 주의 주민들과 회사들의 상업활동을 제한하거나 제한하지 못하게 하려면 어떻게 하여야 하는가 하는 문제들을 다룬다. 구체적인 문제점들을 밝히기 위하여 실지 진행된 법정실례들을 리용한다.

워싱톤주의 스팸방지법

1998년 3월 워싱톤주의회는 《비요청전자우편법》을 만장일치로 통과시켰다. 이 법은 다음과 같이 지적하고 있다.

1. 그 어떤 개인, 회사, 련합체나 협회도 워싱톤주에 있는 콤퓨터로부터 혹은 워싱톤주에 있는 주민이 소유한 우편주소에 상업적인 전자우편의 전송을 할수 없다. 워싱톤주에 있는 주민이나 콤퓨터라고 할 때 그것은;
   - 제3자의 승인이 없이 그 3자의 인터네트령역이름을 사용하는 경우 혹은 정보를 잘못 알려 주어 상업적인 전자우편의 출발지나 전송경로가 틀린 경우
   - 제목란에 허위적인 혹은 오도된 정보를 담은 경우를 다 포함한다.

2. 우편을 받는 사람의 전자우편주소에 포함된 인터네트령역이름의 등록자에게 문의하여 보면 그 령역이름을 알수 있는 경우 개인, 회사, 련합체나 협회는 상업적인 전자우편내용의 해당 수신자가 워싱톤주민이라는것을 아는것으로 된다.

이 법을 어기는 경우 벌금은 전자우편건당 100딸라로부터 1, 000딸라범위로 물어야 한다.

처음으로 제기된 이 법은 워싱톤주의 주민들에게 보내는 비요청전자우편을 완전히 금지시킬수 있었다. 워싱톤주의회는 시민기본권동맹(ACLU)과 기타 의사표현의 자유를 주장하는 여러 단체들로부터 압력이 있었으므로 초심에서 완전금지라는 개념은 철회하였다. 이 법을 반대하는 사람들은 이 법이 《비요청상업적의사표현에 대하여 지나치게 넓은 의미의 정의》를 담고 있다고 보았다. 이러한 거부투쟁으로 말미암아 주의회는 허위적이거나 오도적인 상업전자우편은 금지한다는 식으로 간접적으로 스팸을 통제할것을 결정하였다. 주의회는 이러한 제한조치들이 국가헌법 제1수정조항(언론, 신문, 종교의 자유에 관한 조항임)에 반영된 우려사항들과 보다 상통한다고 보았다.

이 법은 구체적으로 들어 가 스패머들이 흔히 쓰는 두가지 방법들을 금지시켰다.

- 편지출발지나 회신주소가 오도적으로 혹은 부정확하게 된 편지들은 금지시켰다.
- 편지제목란에 허위적이거나 오도적인 정보가 있을 때 그 편지들은 금지시켰다. 스패머들은 흔히 《당신은 벌써 1000딸라를 얻었습니다》 혹은 《당신의 전문분야의 직업을 얻을수 있는 좋은 기회입니다》 등과 같은 글을 제목란에 써넣음으로써 호기심 많은 사용자들이 그 편지를 읽어 보지 않으면 안되게 한다. 만약 전자우편이 이러한 제목이 있어서 일종의 계주식판매전략을 추구하는 경우 그 전자우편은 워싱톤주의 법을 어긴것으로 된다.

이 법은 주의 법이므로 그 범위는 지리적으로 워싱톤주에 제한되여 있었다. 스패머가 그 법을 위반하였다고 판단될수 있는 경우는 오직 그의 콤퓨터가 물리적으로 워싱톤주에 위치하고 있는 경우 혹은 보내는 사람이 받는 사람의 위치가 워싱톤주라는것을 알고 있는 경우이다. 법에 명백히 지적된바와 같이 《받는 사람의 전자우편주소에 있는 인터네트령역이름의 등록자로부터 그 정보를 얻을수 있는 경우》 보내는 사람은 받는 사람이 워싱톤주에 위치하고 있다는것을 안것으로 간주된다.

주검찰총장과 워싱톤주인터네트봉사제공업체련맹(WAISP)은 워싱톤주민들이 가지고 있는 전자우편구좌에 대한 주적인 등록사업을 공동주최하여 진행하였다. 워싱톤주에 있는 전자우편가입자들은 http://registry.waisp.org에 있는 WAISP페지를 접근하여 자기들의 구좌를 등록할수 있었다. 법에 의하면 스패머들은 자기들의 전자우편을 보내려고 하는 대상들에 대하여 WAISP목록을 놓고 대조하여 보고 받을 사람들이 워싱톤주에 살고 있는가를 결정해야 하며 만일 전자우편내용이 주의 법에 어긋나는 경우 그 사용자에게 보내지 말아야 한다.

소송사건의 진상

소송당시 25살쯤 되는 제이슨 헤켈은 오리건주 소재지인 쎄일럼에서 Natural Instinct의 단일소유자였다. 1997년에 헤켈은 《인터네트에서 어떻게 리득을 볼것인가》라는 제목의 46페지짜리 소책자를 하나 써서 인쇄하였다. 그 소책자는 39.95딸라에 팔렸다.

그 도서를 대량 판매하기 위하여 헤켈은 Extractor Pro라는 쏘프트웨어를 리용하였다. 그 쏘프트웨어는 인터네트상에서 전자우편주소들을 찾아 자동적으로 그 주소들에 전자우편을 보내 준다. 도서판매를 촉진하기 위하여 매달 최고 100만통의 비요청전자우편을 보냈다. 이 편지들은 워싱톤주의 사용자들을 포함한 전 세계인터네트사용자들에게 다 보내여 졌다. 소송에서는 매달 약 40부의 책을 팔았다고 제기되였다.

헤켈의 도서판매수법은 스패머들에게서 볼수 있는 전형적인 수법이였다.

- 그는 인터네트상에서 간접적으로 우회적인 경로로 편지를 보냄으로써 편지의 원천지를 알수 없게 하였다.
- 받는 사람들이 회신할 방도를 주지 않았다. 《보내는 사람》란에는 전자우편주소가 없었다. 받은 사람들이 편지내용에 대하여 신소를 하면 주소가 불명확하여 전달되지 못하고 되돌아 오군 하였다. 만일 헤켈의 소책자를 구매하려 한다면 신용카드번호를 가지고 보통우편을 리용하여야 하였다.
- 그는 《이 주소가 맞는지요?》라는 식으로 기만적인 제목을 리용하였다. 이런 제목을 달았으므로 사용자들은 속히워 그 편지가 오래동안 만나지 못했던 친구나 동업자들한테서 온것으로 생각하고 편지를 열어 보게 되였다.

워싱톤주검찰소는 이러한 헤켈에 대한 신소를 여러건 받았다. 그들은 헤켈에게 워싱톤주민들에게 이런 우편을 보내는것을 그만둘것을 요구하는 경고편지를 보냈다. 헤켈이 그에 불복하자 검찰소는 법조항위반으로 그를 워싱톤주최고재판소에 기소하였다.

재판에서 헤켈의 변호사는 이 법자체가 국가헌법의 통상조항을 위반하고 있다고 주장하면서 사건심의를 재판소가 기각할것을 요구해 나섰다. 통상조항은 주와 주사이의 통상에 지나친 부담이 가해 지는 경우 매 주들의 주사이통상규제권한을 제한하고 있다.

2000년 3월 10일 킹현의 상급재판소의 재판장 파커 로빈슨은 헤켈측의 제의를 받아 들이고 주의 법이 위헌적이라고 판결하고 그 소송사건을 기각하였다. 로빈슨에 의하면 그 법은 《적절치 않게 제한적이며 부담적》이다. 이 법은 기업에 부담을 줌으로써 소비자들에게 돌아 가는 리득을 더 적게 하였다. 싸이버공간에서 매 우편접수자가 어느 주에서 사는가를 판단한다는것은 어렵다. 이렇게 되면 《헤켈같은 사람은 50개주의 통상규범들에 매여야 하는데 나는 통상조항에 비추어 볼 때 이것은 문제가 있다고 본다》.

2000년 4월 10일 주검찰총장은 로빈슨재판장의 판결내용을 주최고재판소의 상고심의로 제출하였다. 2000년 7월 현재까지 주최고재판소는 아직 판결을 내리지 못하고 있었다.

주호상간통상조항

독립전쟁이 끝나갈 무렵에 개별적인 주들에서는 자기 주의 리익만 생각하면서 주호상간 및 국제통상을 규제하려고 하였다. 당시의 련맹의회는 국가적인 헌법이 채택되기전까지 각 주들을 대표하는 의회로서 주호상간 통상을 규제할 권한이 없었다. 매 주가 자체의 리익만을 앞세움으로 하여 13가지나 되는 서로 충돌하는 통상규제법안과 세금방책이 새로 련합된 국가를 지배하게 되였다. 이로부터 서로 다른 시장과 관세, 산업들로 하여 주들호상간에 서로 보복하는 현상이 생겼으며 주들사이에는 모순이 커지게 되였다.

1786년 1월 버지니아주의회는 단일한 통상규제체계를 내오기 위한 전국적인 회의소집을 제기하였다. 1787년에 열린 헌법채택대회에서 국회는 《외국과의 통상, 주호상간통상, 인디안종족들과의 통상을 규제》할데 대한 권한을 부여 받았다. 이 통상조항이라고 하는 국회권한이 있음으로 하여 국회는 나라의 경제생활을 규제하며 주경계선안에서는 물론 주호상간통상의 자유로운 흐름을 촉진할수 있는 권한을 가지게 되였다.

자기 주의 활동을 통제하고 규제하려는 주의 권리와 주호상간통상에 대한 통제권을 유지하려는 련방정부의 속심사이에는 자연히 모순이 있기 마련이다. 통상조항의 항목들은 수많은 최고재판소판결이 있지 않으면 안되게 되였다. 최고재판소는 통상조항이 경제와 기업을 규제하는 사실상의 완전한 권한을 국회에 부여하는것이라고 해석하였다. 다음과 같은 여러 요인들을 균형적으로 고려한 후 재판소는 주의회결정을 무효화할수도 있다.

- 주호상간통상에 대한 주규제일치의 필요성과 중요성
- 주호상간통상에 이 규제조치가 주는 부담
- 이 규제조치가 자기 주의 리해관계를 우선시하고 주호상간통상을 경시하는 정도

주들이 지역적관심사로 되는 문제들을 립법화할수 있는 일련의 권한들을 가지고 있는것은 사실이다. 재판소들은 주들이 일정한 형태의 주호상간통상을 규제할수 있는가 없는가를 3가지 조항으로 된 시험을 거쳐 판결한다.

- 이 법이 다른 주를 차별시하지 않는가
- 법의 내용이 전국적 혹은 유일규제조치를 필요로 하는것이 아닌가
- 이 주의 리익이 련방정부의 주호상간통상규제권보다 더 우위에 놓이지 않는가

재판소는 이러한 요인들을 건별로 분석한다. 이 분석을 토의하면서 최고재판소는 이렇게 개괄하였다. 《법조항이 합법적인 해당 지역의 공익이 실시되도록 균형적인 규제조치를 취하여 주호상간통상에 미치는 영향이 단지 우발적인 경우 이러한 통상에 가해지는 부담이 지역리익과 비교해 볼 때 명백히 파도하지 않는 조건에서 그 법을 지지할것이다.》

이 분석적방법의 한가지 실례는 고전적이라고 불리우는 1949년의 련방최고재판소판

결에서 생겨 났다. H.P후드라고 하는 매써츄쎄츠주에 사는 우유공급업자는 뉴욕주에 있는 농민들로부터 우유를 샀다. 그는 그 우유를 매써츄쎄츠주에 있는 공장들에 가져다가 가공하여 주소재지인 보스턴시에서 팔았다. 후드는 뉴욕주 농업 및 시장담당국장에게 새로운 우유가공공장을 꾸리려고 허가를 신청하였다. 국장은 우유가공공장을 건설하면 뉴욕의 우유가 다른 곳으로 흘러 가므로 뉴욕의 우유값이 상승할것이라는 리유로 후드의 청구를 거절하였다.

최고재판소는 자기의 구매자들에게 낮은 가격을 유지할 목적으로 주호상간통상을 단절할 권리가 뉴욕주에 없다고 판결을 내렸다. 이 행동은 주들사이의 자유무역에 하나의 장벽을 쌓아 놓을번 하였다. 어느 주도 세금징수력이나 자기의 경찰력을 동원하여 다른 주의 상품에 대한 경쟁적인 경제장벽을 구축할수 없다. 이런 조치들은 헌법의 통상조항을 위반하는것으로 되며 결국에는 위헌적인것으로 되였다.

법정들에서는 앞으로도 계속 통상조항을 세밀히 분석규정하는 판결들을 계속 내릴것이다. 최고재판소가 헤켈사건이나 다른 주의 류사한 사건을 마침내는 판결할것이다.

헤켈사건의 분석

앞에서도 언급되였지만 로빈슨재판관의 판결은 그 법이 통상조항을 위반했기때문에 위헌적이라고 언급하였다. 그 판결은 싸이버공간의 세계에서는 일반적으로 부정적인 평가를 받았다. 이 비판은 세가지 주요한 요인들에 바탕을 두고 있다.

- 일부 비평가들의 견해에 의하면 스팸이 통상조항의 보호를 받는 주호상간통상의 수준에까지는 이르지 못한다는것이다. 또한 스패머와 우편을 받아 본 사람사이에는 그 어떤 상업적인 거래가 일어 나지 않았으며 단지 비요청적이며 바라지도 않은 전자우편만 있었다.
- 재판관 로빈슨의 견해에 의하면 헤켈에게 있어서 어느 우편접수자가 워싱톤주에 살고 있는가를 결정하는것은 《부담적》이다. 비평가들의 견해에 의하면 헤켈의 스팸을 보내게 하는것은 ISP와 전자우편을 받는 사람들에게 다같이 부담으로 된다는것이다. 헤켈이 자기 편지들을 보낼 《권리》는 결국 ISP가 그 우편을 보관한 보충적인 하드구동기공간을 제공해야 된다는것을 의미한다. 사용자역시 이러한 편지들을 삭제하느라고 많은 시간을 랑비해야 한다. 명백히 보건대 헤켈의 스팸은 ISP와 전자우편사용자들에게 생산성과 추가적인 하드웨어원가의 두 측면에서 부담을 조성하였다.
- 각 주들은 오래전에 벌써 주밖의 원격판매업자들과 잡동사니팍스를 제한하는것과 같은 소비자보호조치들을 법화하였다. 이러한 비요청광고방법과 스팸사이에는 실지 차이가 전혀 없다.

련방재판소에서 이 문제들에 대하여 최종판결을 내릴것이다.

결 론

전문가들은 스팸이 계속될것으로 의견을 같이 하고 있다. 대부분의 인터네트사용자들은 비요청편지 특히 무례한 편지들을 싫어 하고 있다. 스팸은 세계적으로 값눅게 광고하고 편지를 보내는 하나의 방법으로 되였다. 그러나 비량심적이며 사기적인 사람들은 이 방법을 리용하여 이러저러한 모든 제품들을 판매하는데 열을 올릴것이다.

국회의원들, 변호사들, 시민권운동가들, 싸이버공간전문가들은 절도, 사기, 악용건까지 포함하여 비요청전자우편을 제한하기 위한 합헌적인 방법을 계속 탐구해 나가야 할것이다. 법정은 법정대로 스팸으로부터의 어떤 정보의 보호가 통상조항상으로 합헌적인가를 판결할것이다.

참 고 문 헌

1. Patty Wentz, "The War on Spam," *Williamette Week*, November 11, 1998.
2. Wash. Rev. Code §19.190.020 (1998).
3. Peter Lewis, *Spam on Trial*, Seattle Times, June 7, 1998, C1 (quoting ACLU's Jerry Sheehan).
4. Note, *"Washington's 'Spam-Killing' Statute: Does It Slaughter Privacy in the Process,"* 74 S. Wash. L.R. 453 (1999).
5. Wash. Rev. Code §19.190.020(1) (1998).
6. Art. I, 8-3.
7. Peter Lewis, *Anti-spam E-mail Suit Tossed Out*, Seattle Times, March 14, 2000.
8. Peter Lewis, *State Asks Supreme Court to Uphold Anti-Spam Law*, Seattle Times, April 7, 2000.
9. Jethro K. Lieberman, *The Evolving Constitution*, (New York: Random House, 1992) p. 42.
10. *Gibbons v. Ogdens*, 22 U.S. 1 (1824).
11. *Southern Pacific Company v. Arizona*, 325 U.S. 761 (1945).
12. *Pike v. Bruce Church, Inc.*, 397 U.S. 137 (1970).
13. *H.P. Hood and Sons v. DuMond*, 336 U.S. 525 (1949).

제10편
물 리 적 보 안

이 편에서는 정보보안계획이 기초층 즉 물리적보안층이라는 매우 중요한 문제에 대하여 취급한다. 이 편의 두개 장에서는 다 위험평가와 원만한 조종을 실현하기 위하여 전개하여야 할 방법론과 사유과정을 정의한다.

그 과정은 다음과 같다.

1. 시설과 체계환경을 리해하는것
2. 시설들을 부류에 따라 구분하는것
3. 자기가 소유하였거나 임대 받은 시설들의 비중을 고려하는것
4. 보호우선권을 결정하는것
5. 보호필요사항을 결정하는것
6. 핵심적인 자산들을 식별하는것
7. 위험을 분석하는것
8. 자연적인 위협요소
9. 사람에 의한 위협요소
10. 환경에 의한 위협요소
11. 인적요인을 고려하는것
12. 물리적보안의 심리적관계
13. 보안의식과 보안전습
14. 사회공학
15. 기타 위험관리기능들과의 협동

필자 크리스토퍼 스타인커는 다음과 같이 말하고 있다. 《100%안전한것은 없다는 일반적관점에서 보면 정보보안은 보안층의 심부를 리용하여 가장 높은 형태의 보안을 달성한다. 이 층들가운데서 어떤 층에 약점이 있으면 보안은 파괴될것이다. 물리적보호는 정보보안의 계층적과정에서 첫번째 층이다. 만일 그것이 존재하지 않거나 취약하거나 오용된다면 정보보안은 실패할것이다》.

제４３장. 물리적보안은 정보보안의 기초

크리스토퍼 스타인커

물리적보안이란 절도, 간첩행위, 파괴 및 해독행위로부터 사람이나 사물의 안전과 물질적존재를 담보하기 위하여 취해 지는 조치라고 말할수 있다. 정보보안의 견지에서 볼때 이것은 정보, 제품, 사람에 대한 보안을 의미한다.

물리적보안은 가장 오랜 형태의 보안이다. 오래전부터 사람들은 피해로부터 자기자신을 보호해 왔으며 절도나 파괴로부터 자기들의 재산을 보호하여 왔다. 지난날에는 물리적보안이 사람에게 안전성을 지니게 하기 위한 보호가 전부였다. 그러나 기술의 발전으로 물리적보안만으로는 보안효과를 볼수 없다. 정보보안은 각이한 보안층들을 전개하여 자기의 목표를 달성하는 수법이며 때문에 《계층형보안》이라고 하는것이다. 100%안전한것은 없다는 공통된 인식으로부터 출발하여 정보보안은 많은 층을 리용하여 가장 높은 형태의 보안을 달성한다. 이 층들가운데서 어떤 층에서 약점이 있으면 보안은 파괴될것이다. 물리적보안은 정보보안의 계층적방법에서 첫 단계이다. 만일 그것이 존재하지 않거나 취약하거나 잘못 실행된다면 정보보안은 실패할것이다.

물리적보안에 대한 관점과 립장

물리적보안은 아무런 준비없이는 착수할수 없는 련속적인 과정이다. 물리적보안은 반드시 기관의 목표에 부합되여야 하며 정보보안방책에서 제시된 기준과 지침에 따라 적용되여야 한다.

물리적보안의 세계에는 변화가 거의 없으므로(정보보안에서 이여의 통제들처럼 그렇게 빠르지 않다) 그것은 흔히 지루하고 중요치 않는것으로 간주된다. 이 오유로 하여 물리적보안은 종종 소홀히 되거나 되는대로 실행되게 된다. 대체로 정보보안통제의 가장 큰 약점은 통제 그자체가 아니라 통제를 정확히 적용하지 못하는데 있다. 물리적보안에 대하여서는 다른 정보보안의 통제에서와 꼭같은 노력, 꼭같은 힘, 꼭같은 신중성을 기해야한다. 사실 보안통제는 예견성 있고 반복적이며 효과적인 정보보안을 달성하여야 한다.

자물쇠, 경비원, 감시카메라, 식별휘장들은 단순히 물리적보안의 도구와 장비인것이다. 물리적보안을 계획하고 설계하려면 다음의 질문에 대답을 주어야 한다.

- 무엇을 보호하려고 하는가
- 보호할 정보가 얼마나 중요한가(경제적으로, 정치적으로, 사회적안전상으로)
- 누구를 위해 보호하며 그중 어느것이 중요한가
- 무엇으로부터 누구로부터 보호하려고 하는가

모든 곳에서 다 녹스요새(정부의 금괴보관고가 있는 곳)만큼 엄격한 물리적보안이 요구된다고 할수는 없으나 물리적보안은 보호되는 사람과 정보의 중요성에 따라 적용되여야 한다. 이 장에서는 정보보안에서의 일반적인 위협요소와 약점들에 의하여 생기는 위험에 대하여 그리고 물리적보안에서 이러한 위험관리의 기초가 어떻게 마련되는가에 대하여 보기로 한다.

물리적보안의 심리

물리적보안을 계획하고 설계할 때에는 그것이 물리적이면서도 심리학적이라는것을 알아야 한다. 심리학적영향이 가져 올수 있는 좋은점들에 대하여 고려하는것이 중요하다. 가령 물리적보안이 잘 보일수 있게 설계되는 경우(세부내용들은 보이지 않게 보호하면서) 외부침해의 표적이 될수 있는 가능성이 적으므로 자기 기관이 잘 보호된다고 말할수 있다. 이것은 그 기관에 대하여 범죄를 저지르려는 욕망을 제거하기 위한 간접적인 수법의 하나로 된다. 물리적보안의 효과성이 다른 보안통제와 마찬가지로 침습의 기회를 줄이는데 달려 있다면 물리적보안의 심리는 그 욕망을 줄이는데 달려 있다.

시설의 물리적보안

현대작업장의 다양성으로 하여 보편적인 엄격한 물리적보안표준을 수립하는것은 비현실적이다. 그러나 매 장소에서 물리적보안을 잘 보장하는것은 완전하고 안전한 환경을 달성하는데 반드시 필요하다. 이 부분에서는 시설들의 형태를 개괄하고 그것이 어떻게 다른가와 매 시설에 대한 물리적보안에 대하는 방도들을 서술한다.

시설의 구분

시설들은 다음과 같은 일반적인 부류로 갈라 볼수 있다.

- **소유한 시설.** 소유한 시설은 대체로 물리적보안을 유지하기에는 가장 단순한 구조일것이다. 보안관리가 원래 쉬운것은 소유자가 그 시설에 대한 완전한 행정적 관리통제를 가지고 있는것과 관련된다. 이렇게 되면 유연성이 있어 소유자나 관리자가 임의의 물리적보안통제를 임의의 방법으로 하여 보안목적을 달성할수 있게 된다. 소유한 시설의 기본결함은 물리적보안이 파괴되는 경우 소유자가 전적인 책임을 져야 한다는것이다. 소유한 시설의 가장 좋은 실례는 대기업의 본부이다.
- **비소유시설.** 비소유시설은 물리적보호가 좀 더 힘들수 있다. 관리자나 소유자는 물리적보안이 파괴되면 각각 법적책임을 지게 된다. 례를 들어 수도관이 터져

콤퓨터실이 물에 잠기면 콤퓨터실거주자는 소유자가 수도관을 잘 보수하지 못했다는것이 발견되는 경우 그 피해에 대하여 책임을 지울수 있다. 이 경우 비소유시설은 물리적보안파괴에 대한 법적고소대상이 있다는 유리한 점이 있다. 비소유시설의 실례는 건물거주자가 세를 내지만 소유하지 않은 건물 등이다.

- **공유시설.** 공유시설은 대체로 그 형태가 가장 각이하며 위협적인 요소들이 많은 시설들로서 대부분의 구조물들은 이런것들이다. 이 시설들은 하나이상의 시설거주자를 가지며 그중 일부 거주자는 대체로 경쟁자들이다. 그 시설은 모든 거주자들(주어 진 지역에 있는)에게 꼭같은 리용권을 주어야 하기때문에 물리적보호가 매우 힘든것으로 된다. 공유시설의 좋은 실례는 종합청사와 공동청사나 거주자가 많은 비소유시설이 될수 있다.

시설들을 다 구분하면 위험완화전략개발의 첫 단계를 거친것으로 된다. 해당 시설들에 고유한 위협요소들을 리해하면 그것은 그 위협을 방지하기 위한 안목을 가진것으로 볼수 있다. 일부 시설들은 한가지 부류에만 속하지 않으므로 이 구분방식안에 꼭 준하여야 한다는 법은 없다. 여기서 알아야 할것은 이 혼합부류의 시설에서 생길수 있는 새로운 고유한 우단점들이다.

시설의 위치

어떤 종류의 시설을 차지하겠는가에 관심을 가질뿐아니라 그 위치에도 관심을 돌려야 한다. 어떤 장소는 다른 장소보다 더 많은 위험을 내포할수 있다.

다음의 것들은 시설위치를 선택할 때 고려해야 할 위치적인 위협요소들이다.

- **범죄, 폭동, 테로가 생길수 있는 위험성** 고려하고 있는 매 지점들에 대하여 범죄와 테로에 대한 통계자료들을 연구해야 한다. 만일 시설의 위치가 이러한 사고가 빈번한 지대라면 물리적보안이 파괴될 가능성은 커진다. 례를 들어 시설가까이에서 빈번한 시위와 폭동이 일어 나면 시설과 종업원 그리고 고객들을 위협할 우발적인 폭력행위(례: 화제, 범죄 등)가 발생할수 있다. 정보보안에서도 사람의 보호와 안전이 항상 그 무엇보다 우선시되여야 한다.
- **린접건물들과 그 업무종류** 이 부분은 앞에서 언급한 시설의 구분(특히 공유시설) 및 우의 범죄나 폭동의 가능성문제와 관련된다. 자기의 이웃이 누구이며 그들이 무엇을 하는가를 알아 두는것은 좋은 습관이다. 례를 들어 사람들은 경쟁대상들, 원자력발전소 혹은 위험한 화학물질수송로인 고속도도로나 철길옆에 자기 회사의 자료쎈터를 두려고 하지 않을것이다. 또한 이것은 옆에 련결된 건물의 경우도 마찬가지이다. 어떤 사람이 린접건물을 부시고 뛰여 들어 자기 시설에 접근할수 있지 않겠는가, 지붕은 어떤가, 이것들이 다 위치를 선택할 때 제일 먼저 생각해야 할것들이다.
- **비상지원대책** 이것은 비상지원(례: 소방대, 경찰, 의료일군)이 시설에 도착하는데 걸리는 시간으로 간단히 정의된다. 비상지원지점으로부터 시설까지의 운행거

리와 도달시간(가장 통행이 복잡할 때)을 알아야 한다. 이 정보를 알면 비상지원이 도착할 때까지 물리적보안대책들을 실행하여 파괴와 손실을 검출하여 저지시킬뿐아니라 그것을 지원시키고 최소화할수 있다.

- **환경보장** 환경보장은 시설에서 쓰는 깨끗한 공기, 물, 전력이다. 이 모든것들이 앞으로 다 보충될수 있는 여지가 있는가를 확인해야 한다. 특히 가동률이 높은 시설들에 대해서는 두개의 서로 다른 송전망으로부터 전력을 끌어 올수 있는 위치를 선택해야 한다.
- **자연재해의 위험성** 지난 100년간 그 지역에서의 자연재해현상에 대한 지리적 및 기후적통계를 조사하여야 한다. 자연재난은 예측하기 어려우며 완전히 피할수도 없지만 그러한 재해가 보다 적게 일어 날수 있는 지역을 선택함으로써 자연재난의 후과를 최소화할수 있다.

시설에 대한 위협과 통제

이상의 론의내용에서 어떤 위치가 더 많은 혹은 더 적은 위협요소를 안고 있는가를 보았다. 이제부터 위협요소들과 그 통제의 기본형태를 하나씩 보기로 한다. 한가지 위협요소의 근원을 제거할수 있다면 동시에 여러개를 효과적으로 제거할수 있다는것을 보여주자는데 목적이 있다. 뿐만아니라 두 위협요소가 서로 인과관계에 있는 경우 반대현상도 일어 날수 있다는것을 명심해야 한다. 통제는 사실 단순하고 기초적이지만 총체적으로는 해당 위협에 대하여 제지, 검출, 지원, 대응할수 있어야 한다. 위협요소에는 자연적위협요소, 인공적위협요소, 환경파괴의 3가지 종류가 있다.

자연적위협요소 물리적보안이 잘되는 경우 일부 위협요소들에 대하여 심리적안정감을 가지는 우점이 생긴다. 그러나 자연재난은 그렇지 않다. 이 재난을 저지하거나 단념케 할수는 없다. 언제든지 자연환경은 시설에 위협으로 될수 있다. 유일한 방도는 그 영향을 최소화하고 빨리 복구할수 있는 통제를 실현하는것이다. 자연적인 위협요소와 그 일부 통제는 다음과 같다.

－화재는 다음과 같은 위험성을 가지고 있다.
- 열
- 연기
- 억제물(소화기재와 물)의 파괴

－화재통제는 다음과 같이 한다.
- 설비가까이에 연기탐지기를 설치한다.
- 소화기를 설치하고 그 적절한 사용법으로 종업원들을 훈련시킨다.
- 정보체계가까이에서 가스(비액체)소화체계를 리용한다.
- 정기적인 화재소개훈련을 진행한다.
- 모든 예비본매체들을 시설밖에(담보가 있는 제3자에게) 보관한다.
- 재해복구계획을 작성하고 훈련한다.

－불리한 일기조건은 다음과 같은 위험성이 있다.

- 번개
- 강한 바람
- 우박
- 홍수

—불리한 일기조건의 통제대책은 다음과 같다.

- 일기조건의 감시
- 시설을 비바람에 잘 견딜수 있는 장소에 둔다.
- 시설이 정확히 접지되도록 한다.
- 전압안정기와 무정전전원체계(UPS) 혹은 디젤발전기를 설치한다.
- 바닥을 높이 설치한다.
- 정기적인 일기대피훈련을 진행한다.
- 모든 예비본매체들을 시설밖에(담보 있는 제3자에게) 보관한다.
- 재해복구계획을 세우고 훈련한다.

—지진은 화재와 같은 다른 재해를 촉발시킬수 있는것으로 하여 특별히 위험하다. 지진으로 인한 화재에 따르는 추가적파괴뿐아니라 다음과 같은 몇가지 위험이 있게 된다.

- 구급대책기간으로부터 응답이 제한적으로 오거나 전혀 응답이 없다.
- 시설들과 정보체계에 영구적인 구조적, 물리적파괴를 준다.
- 위험요소통제수단이 무효화된다(례컨대 소화기재들을 마비시킨다).
- 사람대피가 제한된다.

—지진에 대한 통제대책은 다음과 같다.

- 정보체계설비를 높은 표면에서 내리워 보관한다(적절한 받침틀이 없이).
- 정보체계설비를 유리창문과 떨어 지게 한다.
- 시설과 그의 하부구조에 지진방지 혹은 진동방지장치를 설치한다.
- 정상적인 지진훈련을 진행한다.
- 모든 예비본매체들을 시설밖에(담보가 있는 제3자에게) 보관한다.
- 재해복구계획을 세우고 훈련한다.

자연환경의 위협은 항상 우에 렬거한것처럼 극적으로 진행되는것은 아니다. 그것은 흔히 훨씬 더 미묘하고 예상외의 형태로 일어 날수 있다. 그 한가지 실례가 건조한 열, 습기 그리고 약한 바람에 오래동안 로출되는것이다. 덜 심각한 이런 위협요소는 사람들에게 즉시적인 경보를 울릴것은 못되지만 그것이 일으킬수 있는 후과는 알아야 한다.

인공적인 위협요소 위협요소의 두번째 부류는 인공적인 위협요소이다. 이 위협요소들은 흔히 사람들의 본성과 련관되는것으로 하여 가장 동적이며 막기 힘들다. 이것은 인공적위협요소들에 악의, 기회, 우연이라는 세가지 자극제가 있는 사실과 관련된다. 인공적인 요소들과 그 몇가지 통제대책들은 다음과 같다.

—절도/사기는 다음과 같은 위험성을 가진다.

- 정보체계기능의 저하 혹은 손실

- 비밀정보나 영업비밀의 손실
- 수입금의 손실

－절도/사기에 대한 통제대책들에는 다음과 같은것들이 있다.

- 건물과 층, 방들이 감시되고 있으며 시설을 드나드는 사람들은 검사받는다는 내용의 표시글을 해당 장소들에 붙여 놓는다.
- 감시카메라들을 볼수 있는 장소들에 설치한다.
- 종업원들속에서 보안 및 안전의식을 높여 준다.
- 식별휘장을 단다.
- 경비원
- 위치표식물의 리용을 최소화한다.
- 정기적인 실사
- 훌륭한 재고관리관계 그리고 재고통제를 엄격히 한다.
- 관건장치를 잘한다.
- 보험
- 직능 및 직무교대의 분리
- 종업원채용/해고방식

－간첩활동은 다음의 위험성을 내포한다.

- 기밀정보나 영업기밀의 손실
- 경쟁력의 손실
- 수익의 손실

－간첩활동에 대한 통제대책들은 다음과 같다.

- 건물과 층, 방들이 감시되고 있으며 시설을 드나드는 사람들은 검사받는다는 내용들을 해당 장소들에 붙여 놓는다.
- 감시카메라들을 보이는 곳에 설치한다.
- 종업원들속에 보안 및 안전자각을 높여 준다.
- 식별휘장을 단다.
- 위치표식물의 리용을 최소화한다.
- 경비원
- 종업원채용/해고방식
- 직능 및 직무교대의 분리
- 정기적인 실사

－태업은 다음의 위험성들을 가지고 있다.

- 정보체계능력의 감소 혹은 손실
- 기밀정보나 영업비밀의 분실
- 수익의 분실

－태업에 대한 통제대책들은 다음과 같다.

- 건물과 층, 방들이 감시되고 있으며 시설을 드나드는 사람들은 검사받는다는 내용의 표시글을 해당 장소들에 붙여 놓는다.
- 감시카메라들을 보이는 곳에 설치한다.

- 종업원들속에 보안 및 안전자각을 높여 준다.
- 위치표식물의 리용을 최소화한다.
- 식별휘장을 단다.
- 경비원
- 보험
- 직능 및 직무교대의 분리

—작업장폭력행위에는 다음의 위험성이 있다.

- 종업원이 상하거나 죽는다.
- 생산력의 손실
- 수익의 손실

—작업장폭력행위에 대한 통제대책들은 다음과 같다.

- 건물과 층, 방들이 감시되고 있으며 시설을 드나드는 사람들은 검사받는다는 내용의 표시글을 해당 장소들에 붙여 놓는다.
- 감시카메라들을 보이는곳에 설치한다.
- 종업원들속에 보안 및 안전자각을 높여 준다.
- 경고표식물의 의식
- 경비원
- 종업원채용/해고방식

사람에게는 재능과 적응성이라는것이 있으므로 인공적위협요소들은 통제하기가 어렵다. 각 기관들은 이러한 위협들에 대처하여 취해 진 통제조치들에 대하여 정기적으로 평가함으로써 자체의 보호계획을 각성 있게 점검해야 한다.

환경적위협요소 위협요소의 세번째 부류는 환경적인 위협요소들이다. 환경적통제조치들은 정보와 그 체계의 운영 및 안전성을 보장하는데서 중요하다. 깨끗한 공기, 물, 동력 그리고 믿음직한 온습도조절장치들이 없다면 정보체계는 일관성 있게 운영되지 못하고 완전한 파괴를 당할수도 있다.

—온습도파괴는 다음과 같은 위험성을 가져 온다.

- 시설과 하부구조가 과열로 하여 오동작 혹은 고장이 생긴다.
- 보존매체나 예비본매체가 파손된다.
- 기밀설비요소가 파손된다.

—온습도파괴의 통제대책들은 다음과 같다.

- 정보체계설비의 온도를 감시한다.
- 정보체계설비가 있는 모든 방들에서 합리적인 온도 10～25℃를 유지한다.
- 습도를 20～70%로 유지한다.
- 정보체계설비가 있는 방에서 불필요한 조명장치들을 끄도록 한다.
- 온습도조절체계의 정상적인 점검과 감시를 진행한다.
- 모든 예비본매체들을 외부에(담보가 있는 제3자에게) 보관한다.
- 재해복구계획을 작성하고 훈련한다.

—물과 액체류출은 다음의 위험성을 내포한다.

- 시설과 하부구조가 물이나 다른 형태의 액체에 지나치게 접촉하여 고장이 나는 경우가 있다.
- 보존/예비본매체와 중요한 종이서류로 된 정보가 손상된다.
- 중요한 설비요소들이 손상된다.

—물과 액체류출에 대한 통제대책들은 다음과 같다.

- 시설가까이에 방수포를 준비하여 둔다.
- 중요한 정보체계설비가 있는 방들에 물빼기시설, 물수감기를 설치하고 바닥도 높여야 한다.
- 상하수도관을 정기적으로 검사한다.
- 정보체계가까이에서는 기체소화기를 리용한다.
- 모든 예비본매체들을 외부에(담보가 있는 제3자에게) 보관한다.
- 재해복구계획을 작성하고 훈련한다.

—정전은 다음과 같은 위험성을 가진다.

- 중요한 설비요소가 파괴된다.
- 쏘프트웨어와 기억/예비본매체들이 파괴된다.
- 온습도조절장치가 손상된다.
- 물리적접근조종장치들이나 감시기구의 손상(례: 감시촬영기, 출입문경보장치, ID카드읽기장치).

—정전통제장치들은 다음과 같다.

- 무정전전원장치나 디젤발전기를 설치한다.
- 자동안정기를 리용한다.
- 전압파동을 조종하기 위한 전원단려파기를 설치한다.
- 정전기차단장치와 대전방지수단을 쓸수 있으면 설치한다.
- 모든 설비가 정확히 접지되였는가를 확인한다.
- 회로 및 도선을 정기적으로 검열한다.
- 두개의 서로 다른 송전만으로부터 전력을 끌어 온다(가능하다면).
- 모든 예비본매체들을 외부에(담보가 있는 제3자에게) 보관한다.
- 재해복구계획을 작성하고 훈련한다.

환경적파괴는 그자체만으로도 정보체계에 상당한 손상을 줄수 있는 위협요소이다. 그러나 환경적인 조건의 파괴는 또한 자연적 혹은 인공적인 요인에 의해서도 나타날수 있다. 그러므로 방어심도가 깊은 계층적인 방법으로 모든 위협을 대하는것이 중요하다. 그래야 대부분의 위협요소들을 다 통제할수 있을뿐아니라 그 통제수단들이 그 포괄범위에 있어서도 철저성이 보장된다.

시설보호전략

물리적보호를 위한 전반적인 전략을 작성하는것은 정보보안을 성과적으로 실현하는

여러 단계들중의 하나이다. 보호전략에는 방책들이 여러가지가 있을수 있으며 그러므로 어느것이 더 큰 중요성을 가지는가에 따라 정보의 비밀성, 무결성, 리용성중 어느 하나가 중요시될것이다. 구획화(zoning)는 효률적이며 효과적인 정보보호를 위한 물리적토대를 구축하는 한가지 전략이다.

구획화. 구획화는 새로운 개념이 아니다. 전통적으로 구획화란 숨겨 진 위치(천정우, 지하 등)에 있는 불이나 연기를 알아 내는 화재감시경보기를 설치하는데 쓰이는 하나의 공정을 말한다. 또한 지금까지 호상구획화(cross–zoning)라는 개념이 쓰이였는데 그것은 둘 혹은 그이상의 경보기들이 울리게 함으로써 허위경보를 줄이게 한다.

구획화는 매우 유연하며 가장 단순한것으로부터 가장 구체적인 보안모형에도 다 리용된다. 이로부터 다른 모든 물리적보안통제수단들(례: 움직임탐지기, 물리적침입탐지경보기, 감시카메라 등)에도 이 구획화개념을 적용할수 있다. 가장 큰 우점은 역할에 기초한 접근조종모형이라는데 있다. 역할에 기초한 접근조종방식에서는 사용자들이 기관에서의 자기들의 역할에 따라 체계, 정보 그리고 물리적지역에 대한 접근권을 부여 받는다.

그림 43－1은 역할에 기초한 접근조종을 위한 구획화의 기초적인 실례를 보여 준다. 이 실례에서 1구획부터 4구획까지 표식되며 4는 가장 제한이 크다. 이 시설에서 매개 종업원은 1, 2 및 3지역에 대한 접근권을 가지지만 정보기술부장, 정보기술부원들 그리고 보안관리자는 자신들의 역할로 하여 1, 2, 3 및 4지역에 대한 접근권을 가진다.

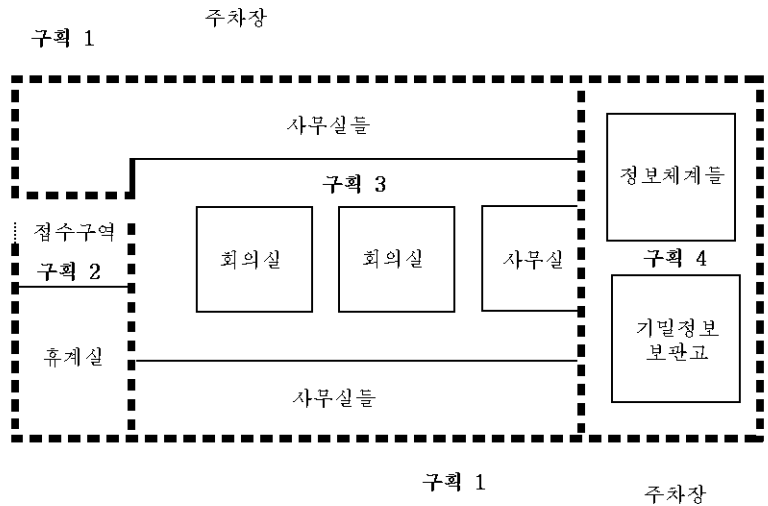



그림 43－1. 역할에 기초한 접근조종의 구획화

보안이 점진적이라는것은 명백하다. 시설의 보다 깊은 곳으로 들어 갈수록(왼쪽에서 오른쪽으로) 구획들은 더욱 제한성을 가진다. 일단 이것이 완성되면 다음 단계는 접근통제구획들에 설치하여야 할 통제기구들을 결정하는것이다. 보다 제한적인 구획일수록 통제가 보다 강하고 믿음직해야 한다는것을 명심해야 한다.

물리적접근조종과 역할에 기초한 통제 그리고 구획화를 결합하면 정보와 재산을 물리적으로 보호하는 철저하고도 중앙집권적인 체계를 세울수 있다. 구획화는 정보보안전략에서 매우 중요한 부분으로 될수 있다. 그러나 구획화실시에 앞서 먼저 위험분석(재산에 대한 위협들과 약점의 리해)을 하여야 하며 위험축소전략을 세워야 한다. 오직 그때에만 구획화는 기관의 정보보안목표를 달성할수 있는 견고한 기초를 마련할수 있을것이다.

정보체계의 물리적보안

물리적보안의 둘째 부분은 정보체계에 대한 물리적보호이다. 이미 언급한것처럼 보호는 계층적이여야 한다. 만일 기관의 콤퓨터가 단 한대라도 물리적으로 그 무결성이 손상된다면 정보체계는 위험에 빠질수 있다. 만일 어떤 사람이 한 콤퓨터에 비법적으로 물리적으로 접근한다면 그 사람은 그 콤퓨터의 모든 정보들에 대하여 지어는 그 콤퓨터와 련결된 다른 자원들(파일봉사기, 메인프레임전자우편 등)에 대해서도 접근할수 있다.

정보체계의 분류

정보체계는 세가지 형태로 분류할수 있다.

- **봉사기/메인프레임** 보통체계에서 물리적으로 가장 안전한 부류이다. 그것은 이 체계들을 일정한 형태의 접근통제와 환경통제가 있는 위치에 두는것과 관련된다. 이 형태가 비록 가장 안전하다 하더라도 그 전반적인 보안은 그것에 접근할수 있는 워크스테이션과 휴대형장치들의 물리적보안에 달려 있게 된다.
- **워크스테이션** 보통시설에서보다 열린 지역, 보다 접근하기 쉬운 장소에 위치하고 있다. 일하는 곳에서 쉽게 사용할수 있는것으로서 워크스테이션들은 주의해서 쓰지 않으면 물리적보안문제를 일으킬수 있다.
- **휴대형기구** 기관의 보안상 큰 골치거리로 될수 있다. 비록 종업원들에게 무릎형콤퓨터와 PDA를 공급하는것이 기관의 유연성과 생산성을 높이기는 하지만 그것은 물리적보안상 몇가지 심각한 위험성을 안고 있다. 임의의 장소에서 회사의 내부정보체계에 사용자들이 들어 올수 있는것과 함께 어느 한가지의 휴대형기구에서 물리적보안이 위반되면 기관의 정보보안이 크게 뒤흔들릴수 있다. 이 부류에 극도의 주의를 돌려야 한다.

정보체계에서 물리적위협과 그 통제방법

정보체계를 분류하면 어떤 위협이 어느 체계에 대하여 더 큰 손실을 주는가를 쉽게

결정할수 있다. 이렇게 되면 통제수단을 어떻게 적용하겠는가에 대한 방향이 서게 된다. 아마 정보체계에 대한 가장 큰 위협은 사용자들의 위협일것이다. 만일 어떤 사용자가 자기의 콤퓨터를 물리적으로 보호하는데 응당한 노력을 기울이지 않으면 거의 모든 통제수단이 무력하게 되고 그 장치는 결국 위험하게 될것이다. 이 부분에서는 정보체계에 대한 기초적인 위협요소들과 그 통제수법들을 개괄한다.

—손실/절도/파괴는 다음과 같은 위험성을 가진다.

- 기밀정보나 영업비밀의 손실
- 생산의 손실
- 수익의 손실

—손실/절도/파괴에 대한 통제방법

- 장치들에 대한 물리적인 관건장치
- 장치에 표식과 딱지붙이기
- 위치표식물리용의 최소화
- 기밀정보보관의 암호화
- 기밀정보들에 대한 자료분류와 처리절차
- 보험
- 정보보안의식화교육
- 감시카메라를 보이는 곳에 설치하기
- 경비원
- 경보체계
- 정기적실사

—비법접근은 다음과 같은 위험성을 가진다.

- 기밀정보나 영업비밀의 손실
- 정보를 마구 변경하는것
- 부정쏘프트웨어
- 수익손실

—비법접근에 대한 통제방법

- 조종탁관건장치
- 좋은 암호를 잘 사용하는 습관
- 정보보안의식화교육
- 기밀정보에 대한 자료분류와 처리절차
- 위치표식물리용의 최소화
- 감시카메라를 보이는 곳에 설치하기
- 기밀정보보관의 암호화
- 강력한 인증조종 및 접근조종

보안의식화교육

비록 오늘 세계적으로 정보체계가 전례없이 널리 리용되지만(앞으로 더욱 그렇게 될것이다) 우리는 여전히 물질적인 세계에서 살고 있다. 모든 종업원들이 물리적보안에 영향을 주며 그것은 기관의 정보보안에 직접적으로 영향을 미친다. 일반적으로 물리적보안이 파괴되는것은 통제수단을 대다수의 종업원들이 모르기때문인것이다. 모든 종업원들에게 정상적으로 강습을 주는것은 본의아닌 보안우회를 줄이는 한편 위험을 완화하기 위한 경제적인 방도로 된다. 정보보안계획이 얼마나 잘 설계되고 실현되였든 관계없이 모르는 종업원이 한명이라도 있으면 보안이 다 파괴되게 된다. 물리적보안은 반드시 의식화계획에서 하나의 제목으로 되여야 하며 다음과 같은것을 포함해야 한다.

- 모든 종업원들에게 그들이 물리적보안에 대하여 조금만 홀시해도 얼마나 빨리 정보보안사고가 나며 혹은 생명을 잃는데까지 이르게 되는가를 보여 주어야 한다.
- 종업원들을 기관의 보안기준과 지침에 기초하여 교육해야 한다. 종업원들이 그에 대하여 응당한 책임감을 가지게 해야 한다.
- 정보보안과 관련된 월간출판물을 모든 종업원들에게 배포해야 한다. 거기에서 물리적보안을 정기적인 화제로 취급해야 한다.
- 경영진에 특별한 방향을 제기하여 순회시찰도 하게 함으로써 정보보안이 어떻게 실행되는가를 막뒤에서 보게도 하여야 한다. 이것은 지지를 불러 일으킬것이다.

의식화에 시간과 노력을 들이는것은 개인의 물리적보안뿐아니라 전망적인 정보체계의 효과성을 높일것이다. 종업원들이 자기의 책임을 알게 하면 그들속에서 주인다운 자각과 의무감을 불러 일으킬수 있다. 이것은 사람들이 가지고 있던 보안상 불리한 점을 유리한 점으로 전환시킨다.

요 약

물리적보안은 정보보안에서 적지 않은 지위를 차지한다. 일부 경우에 기관들은 훌륭하고 강력한 물리적보안을 갖추지만 정보보안의 다른 많은 요소들이 부족하다. 정보보안실천자들은 반드시 그 범위를 리해해야 하며 자산을 보호하기 위해 물리적보안을 어떻게 리용해야 하는가를 잘 알아야 할것이다. 완벽한 물리적보안은 모든 재산을 보호할뿐아니라 다른 형태의 보호를 구축할수 있는 훌륭한 기초를 마련해 줄것이다. 물리적보안이 정보보안의 기초라는것은 명백하다.

참 고 문 헌

1. Fennelly, Lawrence J., et al. *Effective Physical Security, second edition,* Butterworth-Heinemann, 1997.
2. Fites, P. and Kratz, M.P.J., *Information Systems Security: A Practitioner's Reference.* International Thomson Computer Press, 1996.
3. Tipton, Harold and Krause, Micki, Eds., *Information Security Management Handbook,* 4th edition. Auerbach Publications, 2000.
4. Department of Education, National Center for Education Statistics, *Protecting Your System: Physical Security* (online), 1998. Available from World Wide Web: (http://nces.ed.gov/pubs98/safetech/chapter5.html).
5. Tipton, Harold and Krause, Micki, Eds., *Information Security Management Handbook,* Auberbach Publications, 1999.
6. Linux Documentation Project, *Security How-To: Physical Security* (online). Available from World Wide Web: (http://www.linuxdoc.org/HOWTO/Security-HOWTO-3.html).

제４４장. 물리적보안

브루스 아르 매슈

Security (si kyoore'te) n., pl. －ties 1. 안전감을 느낌; 공포, 의심 등에서의 해방, 2. 보호; 보호수단

웹스터사전의 이 정의는 보안실천가들을 위하여 접근조종이라고 다시 정의할수 있다. 정보기술보안실천가들의 모든 사업측면은 사실 정보에 대한 접근을 정의하고 실천하며 감시하는 과정의 련속이다. 여기에는 물리적인 접근도 포함되여 있다. 물리적인 보안을 언제 얼마나 리용하며 그것을 전통적인 정보기술보안에 어떻게 가장 잘 결합시키겠는가 하는 문제들은 IT보안전문가들이 알아야 할 개념들이다. IT보안을 전공한다고 하여 반드시 기술전문가가 되여야 할 필요는 없다. 기술전문가는 다른 사람들이 할수도 있는 일이지만 보안방책과 전략들이 잘 세워 지자면 물리적보호의 장점은 물론 단점들까지도 고려해야 한다. 성공하는가 못하는가 하는것은 물리적인 보안담당자들과 긴밀히 협조하는데 달려 있다. 그들은 정보기술보안이상의것을 알고 있기때문에 서로가 하는 사업들을 호상 존중해 주면 사업이 더 잘되여 나갈수 있게 된다. 특히 사고가 나는 경우 같은 때에는 서로 강습을 진행하면 크게 도움이 될수 있다. 본질상 계층적이며 학과적인 보안을 실현하면 안전한 느낌을 가지며 공포와 의심에서 해방될수 있다. 통제적인 접근이 곧 보안이다.

보안은 접근조종이다

보안이라고 하면 흔히 실현의 견지에서만 보안을 생각한다. IT보안에서는 통과암호와 방화벽이 떠오른다. 개인신상보안에서는 어두운 골목길, 수상한 자들을 피함으로써 강간이나 강탈을 피하는것이 떠오른다. 그러나 IT보안의 견지에서 물리적보안을 고찰하려면 보안을 어떻게 실행하는가 하는 문제보다도 보안이란 무엇인가를 잘 알 필요가 있다. 가장 간단히 말하면 보안은 결국 접근조종이다. 따라서 보안실현이라고 하는것은 접근을 조종 혹은 통제하는 과정이다. 통과암호와 방화벽들은 망자원들과 자료자원들에 대한 접근을 통제하는 역할을 한다. 어두운 골목길이나 수상한자들을 피하는것은 우리의 생명과 소지품에 대한 접근을 통제하는 역할을 한다. 마찬가지로 주택에서의 보안은 출입문들과 창문들에 잠그는 관건장치들에 귀착된다. 이 관건장치들이 있음으로 하여 보호구역에로의 사람들의 접근을 통제하는것이다. 정확한 열쇠를 가지지 않으면 누구든 들어 갈수 없게 되여 있다. 필요한 사람에게만 열쇠를 줌으로써 접근을 통제하는것이다. 최근에 가정용경보장치들은 인기가 더욱 높아 지고 있다. 이 장치들도 역시 은밀한 방법으로 집에

침입하는자들의 행동을 제한함으로써 접근을 통제조종한다.

보안이 접근조종이라는 이 정의는 우리가 잘 알고 있는 정보보안의 기본개념인 리용성, 무결성, 비밀성개념들에도 그대로 적용된다. 리용성은 필요한 경우에 자료에 대한 접근을 담보하는것이다. 무결성은 자료가 변경되지 않았다는것을 의미한다. 그렇게 함으로써 자료변경을 위한 접근권은 합법적인 사람이나 프로그람에만 한정된다.

비밀성은 정보를 인증 받은 사람에게만 보이도록 한다는것이다. 결국 비밀성은 자료를 읽기 위한 접근을 조종한다. 이상의 모든 개념들은 서로 다른 측면에서 자료에 대한 접근을 조종한다. 리상적으로 보면 안전담보란 접근에 대한 조종의 정도와 같다고 할수도 있다. 그러나 현실세계에서는 그 담보가 사람들이 통제수단들을 얼마나 신뢰하는가 하는 정도와 같다고 하는것이 더 정확하다. 높은 수준의 담보는 접근조종수단들이 은을 내고 있다는 높은 수준의 신심, 믿음과 같다. 례를 들어 창문에 관건장치를 하는것은 중간정도의 담보만을 준다. 그것은 결심을 품은 침입자가 창문을 쉽게 깰수 있다는것을 알고 있기때문이다. 그러나 침입자가 유리를 깨는 소리에 의해 발각될수 있으므로 어느정도 접근조종이 담보된다.

접근이 적다고 하여 보안이 언제나 더 잘 보장되는것은 아니라는것을 명심해야 한다. 즉 접근조종은 접근거부와 다르다. 창문에 쇠를 잠그는것은 총체적으로 접근거부를 위한 하나의 통제수단이다. 실지 모든 통제수단들은 완전접근과 완전거부사이의 구간에서 실시되는것만은 명백하다. 그렇기때문에 보안을 보장하는것은 접근의 량이 아니라 접근조종의 수준이다. 그러한 통제수단들에 대한 신뢰도에서 곧 담보가 나오게 된다.

이로부터 계층적방어라는 다음의 화제가 제기된다.

계층적방어

계층적방어는 보호를 일정하게 여유 있게 확대함으로써 접근조종에 대한 신뢰도를 높여 준다. 물리적보안을 위한 계층적방어의 세부설계는 이 장에서 취급할 내용이 아니므로 경험 있는 물리보안전문가에 의하여 다루어 져야 할 문제이다. 그러나 정보기술보안전문가는 계층적방어의 우점과 그것이 보안에 주는 영향을 평가할수 있어야 한다. 계층적방어의 설계를 위하여 필자는 범위, 심도, 억제라는 세가지 원칙을 제기한다.

범위의 적용을 하나의 벽에 구멍들을 여러개 뚫는것으로 생각하자. 매개 구멍들은 여기서 서로 다른 취약점들을 나타낸다. 단 한가지의 통제수단이 이 모든 취약점을 제거할수 없으므로 여기에 범위개념이 리용된다. 먼저 이것을 누구나 다 알고 있는 정보기술세계와 련관시켜 보자. 한 사람이 접속개시암호(단어)로 자료에 대한 읽기접근을 통제하기로 결심하였다고 하자. 그러나 접속개시통과암호는 인터네트로 전송되면 보호 받을수 없다. 그러므로 다른 형태의 통제수단(례: 암호화)이 추가적으로 요구된다. 물리적보안은 꼭같은 방법으로 동작한다. 례를 들어 단층짜리의 자그마한 제품창고에 있는 상시대기실에 대한 접근조종이 필요하다고 가정하자. 그 시설에는 앞문, 뒤문, 큰 차고문, 그리고 열지 못하는 고정창문들이 있다. 출입문들에 있는 관건장치들은 내부에로 들어 가는 하나

의 통로만을 통제하지만 깨질수 있는 창문들에 대한 보호는 제공하지 못한다. 결국 창문에 빗장을 질러 주어야 전반적범위에 대한 완전한 방어를 할수 있게 된다.

둘째 원리인 심도는 흔히 계층적방어에서 가장 중요한 측면임에도 불구하고 무시되군 한다. 보안이 실천적으로 되자면 반드시 실패도 맛 보아야 한다. 그 어떤 통제수단이라도 완전한것은 없으며 언제든지 파손될수 있다. 그러므로 심도를 보장하기 위하여 추가적인 접근조종계층들을 뒤선에 덧치는것이다. 본질에 있어서 하나의 벽이 여러개의 벽으로 겹겹이 된 셈이다. 류사한 문제로서 사용자통과암호를 보자. 통과암호는 영원히 비밀로 될수는 없으며 지어 하루도 비밀로 되지 못하는 경우까지 있다. 그것은 사용자들이 통과암호를 어디에 써놓거나 공유하는 습관이 있기때문이다. 걱정할 필요는 없다. 아무리 교양과 훈계를 하여도 통과암호체계가 잘못될수 있다는것은 다 아는 사실이다. 그러므로 《몸에 지니고 있는것》, 《머리속에 알고 있는것》, 《신원으로 될수 있는것》을 리용하게 된다. 우리가 흔히 쓰는 통과암호는 《머리속에 알고 있는것》의 부류이다. 나머지것들은 인증체계에 일정한 정도의 심도를 추가적으로 보장해 준다. 《몸에 지니고 있는것》인 스마트카드와 같은 추가적인 보호층을 부가하면 심도가 실현된다. 이렇게 되여야 통과암호 하나가 로출되여도 접근조종은 여전히 가능할수 있다. 그러나 스마트카드에도 역시 재현성이 있으므로 통제수단검증을 위한 실사를 꼭 하여 수복하여야 물리적보안이 다시 자기 궤도에서 보장되게 된다.

물리적보안에서 심도는 보통 바깥경계선 즉 보호하려는 대상으로부터 멀리 떨어 진 구역에서부터 그 대상가까이의 중심구역으로 들어 오면서 보장되여야 한다. 리론상 접근조종의 매개 계층은 동심원을 이룬다(비록 완전히 둥근 시설은 없지만). 매 계층에 대한 구획은 흔히 마당의 울타리, 건물입구와 바깥면, 건물의 매 층, 통합사무실들, 개별사무실, 서류장 및 서류금고로 갈라 본다.

셋째 원칙인 억제는 충분한 통제수단들을 배치함으로써 잡히지 않으면서도 그것들을 파괴하는것을 목표로 노린 대상물의 가치보다 더 원가가 들거나 타당성이 없게 하는것이다. 만일 훔쳐야 할것이 5,000딸라짜리 예비용봉사기인데 뒤골목에서 팔면 1,000딸라밖에 못받는다고 하자. 이런 경우 한 종업원이 가만히 숨어 들어 와서 그 기계를 뒤문으로 내가는데 이때 뒤문에 감시카메라가 있어서 앞으로 직업을 잃고 감방에 갇혀 있는 기간에 5, 000딸라가 소요될것 같으면 훔치는 노릇이 수지 맞지 않게 된다. 여기서 억제요소는 회사가 아니라 그 종업원에게 값을 치르게 한다는것을 명심하라. 그런데 흔히 물리보안전문가들은 소유자에게만 돈이 드는것으로 잘못 생각하는 경향이 있다. 보호원가 대 재해복구/교체원가사이의 관계를 분석하는 위험분석때에는 보호대상에 대한 소유자의 투자값이 필요하다. 5, 000딸라짜리 기계를 지키려고 10, 000딸라를 들이려는 사람은 없을것이다. 그러나 억제라는 원칙에서는 범죄자들의 능력 대 비용의 관계 즉 범죄자자신이 내적으로 진행하는 위험평가에 대하여서도 반드시 고려에 넣어야 한다. 이 경우 1만딸라짜리 감시카메라체계대신 300딸라짜리 비감시카메라를 뒤문에 설치해도 충분할것이다.

여기서 난점은 계층적방어가 어느 부분이 범위와 심도이고 어느 부분이 억제인가를 결정하는것이다. 그렇기때문에 매 계층이 탐지, 억제 혹은 지연에 어느 정도로 기여하는가를 세밀히 분석하여 한 위험요소의 동기와 능력도 계산해 보아야 한다. 이러한 통합적인 대안은 수지를 맞추는 과정으로서 분석적위험관리라고 부른다.

물리적보안기술

보안구성요소

관건장치 물리적보안통제수단들은 대체로 관건장치로 구성된다. 기능상으로 보면 낮시간접근자물쇠, 근무시간외자물쇠, 비상출구자물쇠가 있다. 낮시간자물쇠는 번호판이나 카드읽기장치와 같은것으로서 해당 인원들의 출입을 위한것이다. 근무시간외자물쇠는 자주 열거나 채우게 되여 있지 않으며 보다 견고하다. 비상출구자물쇠는 한 방향으로의 움직임(즉 화재대피시 사용)에만 쓰고 다른 방향으로는 가기 힘들게 되여 있다.

류형상으로 보면 관건장치들은 기계적인것도 있고 전자적인것도 있다. 기계적관건장치들은 전기를 쓰지 않는다. 일상적으로 쓰는 대부분의 관건장치들은 기계적인것들이다. 전기적관건장치는 유도선륜이라고 하는 잠금장치를 움직이는데 전기를 쓴다. 유도선륜은 철심둘레에 코일을 감은것이다. 철심은 코일에 전류를 통과시키면 안팎으로 움직이게 되여 있다. 다른 전기쇠형식은 커다란 전자석을 리용하여 문을 닫아 매는것이다. 이것의 좋은점은 움직이는 부분은 거의 없이 문을 잡는 힘이 매우 센것이다.

사람들이 관건장치의 인증(IT용어를 사용한다면)을 받는 방법은 날이 감에 따라 더욱 더 복잡해 지고 있다. 전통적으로 사람들은 일반열쇠나 기계열쇠를 썼다. 지금은 번호판을 돌려 내부극소형처리기와 회로에 전원을 투입하여 여는 번호관건장치들도 있다. 또한 전자수자판, 콤퓨터, 생체계측값, 카드열쇠로 사람들을 식별하는 방법들도 있다. 이것들이 IT보안전문가들에게는 보다 익숙된 .분야로 되지만 쥐여 짜면 결국에는 다 같은 관건장치이다. 총체적으로 문관건장치와 결합된 인증체계를 《출입문조종체계》라고 한다.

장벽 장벽에는 바람벽, 울타리, 출입문, 문주, 정문이 포함된다. 장벽설계에는 실로 놀랄만한 량의 기술과 사유가 필요하다. 장벽설계의 계산에는 폭탄폭발과 화재견딤성, 폭력적용가능성이 다 들어 간다. 장벽설치에서 고려해야 할 문제점들에는 바닥충진과 바람견딤성이며 미학적측면도 역시 고려해야 한다. 수많은 선택사항들을 맞추자면 다음의 문제 즉 《장벽이 누구 혹은 무엇을 저지하기 위한것이며 얼마동안 필요한가》라는 문제에 대답이 주어 져야 한다.

이에 대한 답을 주자면 장벽을 하나의 접근조종요소로 보아야 한다. 사무실에 들어 가는 문이 아니라 사무실에 들어 가는 사람 또는 사물을 통제하기 위한것이 바로 이 장벽인것이다. 예비본테프와 같은 귀중한 자료들이 사무실에 있는가, 하드웨어도난과 같은 것을 방지하자는것인가, 예상되는 도적이 회사사원인가, 침입이 가능한 장소가 작은 사무실들인가, 그 사무실이 목재건물이여서 화재에 의한 자료손실이 기본위험으로 되고 있는 곳인가 만약 그렇다면 화재는 접근 못하도록 얼마나 견제될수 있는가(즉 소방대대응소요시간은 얼마인가) 등에 대한 질문이 제기되고 그 해답들이 나와야 한다.

경보장치 장벽과 관건장치들은 접근조종을 직접 실현한다. 그러나 경보는 그러한 통제수단들이 제대로 작용하는가 즉 접근조종이 위반되였는가를 알려 주는것이 일차적목적으로 되고 있다. 경보는 대개 사람이 어떤 행동을 취해야 한다는것을 알려 주는것이다. 화재경보는 물살포기를 자동적으로 투입하면서도 소방대에 의한 사람의 대응도 촉구해

준다. 계층적방어의 관점에서 보면 경보기가 있음으로 하여 억제력이 추가된것이나 같다. 수감부는 침입자의 움직임이나 화재의 열 등 경보조건들을 수감하여 조종체계에 보고하면 조종기는 대응을 시작하여 경보종을 울리든가 경찰에 비상전화를 거는 등의 대응조치들을 취한다. 여러 통제장치들을 감시하는 시설을 가리켜 《중앙감시》시설이라고 한다.

우에서 이야기된것과 같이 수감부들은 흔히 환경조건이나 침입을 탐지한다. 환경적조건에는 온도, 습도, 진동이 있다. 온도수감으로는 화재경보뿐아니라 봉사기방에 있는 공기조화기의 고장도 알수 있다. 습도수감으로는 비나 수도관이 터져서 생기는 침수를 알수 있다. 진동수감부는 환경수감부들과 같이 리용하여 중요한 하드웨어들을 보호할수 있을뿐아니라 유리파손수감부 같은 침입수감부에도 쓰이며 울타리에 설치하여 누가 울타리에 기여 올라 오는가 하는것도 탐지할수 있다. 기타 침입수감부로는 방안의 초음파나 열의 변화를 계측하여 사람의 움직임을 탐지할수 있다. 사실상 침입수감부들의 대부분은 인간활동에 맞게 설정된 환경수감부들에 지나지 않는다. 따라서 전기를 끄지 않은 커피끓이개나 실내선풍기들과 같은 제품들도 허위경보를 울릴수 있다.

출입문들에는 자석스위치들이 설치되여 있어 감시가 진행된다. 문에는 자석을 설치하고 얇은 철띠들로 만들어 진 스위치가 문틀에 설치된다. 문이 닫기면 자석이 철띠와 맞붙어 문을 꼭 닫게 해주어 회로가 구성된다(열면 회로가 끊어 진다).

울타리주변감시는 마이크로파나 적외선광속으로 하는데 이 광속은 사람이 들어 오면 끊기면서 경보가 울리게 되여 있다. 케블을 지면에 묻어 두고 사람들이 지나 가는것을 탐지한다. 동물들이 지나 가면 이 주변감시장치들이 오유경보를 울리군 한다.

이 수많은 경보체계에서 중요한 특징은 유선이나 무선으로 어떻게 수감장치들과 조종체계에 련결시키는가 하는것이다. 무선체계들은 설치하기 쉬우나 라지오파장애나 인위적인 전파장애의 영향을 받을수 있다. 유선체계들은 비용이 많이 들거나 설치하기가 힘들지만 도관에 묻는 경우는 매우 안전하다. 유선이든 무선이든 조종장치가 그 체계들의 무결성을 감시하게 되면 더 좋다. 수감부들에 조작스위치들을 달고 《선로감시》를 통하여 통신선결선상태를 확인할수 있으면 더욱 좋다.

경보에서의 기본문제는 경보장치가 누구와 무엇을 탐지하게 되여 있는가, 대응행동은 무엇인가이다. 여기서 《누구》인가에 의하여 경보체계의 정교화가 결정된다면 《무엇》인가에 따라 수감장치들의 예민도가 결정될수 있다. 이것들이 결정되면 경보전문가는 수감부들을 적당히 섞어 배치할수 있을것이다.

경보조종기가 기본적으로 하는 일은 수감기들에서 들어 오는 정보에 따라 경보체계들을 가동시키거나 끄는 일이다. 이러한 주요한 기능을 가지고 있기때문에 그것을 끄자면 그러한 사람의 권한을 인증할수 있는 수단이 있어야 한다. 앞에서 언급된것처럼 이런 인증을 하는 방법은 본질상 통과암호로부터 시작하여 스마트카드, 생체계측정보에 이르기까지 임의의 정보체계의 인증방법과 꼭같으며 모두가 우단점이 다 있다.

조명과 카메라 조명과 카메라를 결합하는것은 본질상 꼭같은 기능 즉 사람이 보게끔 하자는것과 관련된다. 더우기 조명은 카메라에 있어서 없어서는 안될 요소이다. 빛이 너무 세거나 너무 약하면 자동차처럼 큰것도 볼수 없게 된다. 카메라조명을 적당히 하는것은 쉬운 문제이지만 높은 보안조건에서는 조명기재제작업체와 카메라제작업체에 자료를 의뢰하여 받을수 있다. 일반적으로 카메라가 침입자를 탐지할수 있다고 잘못 생각할

수 있다. 카메라도 탐지할 가능성은 있다. 억제력의 견지에서는 조명과 카메라가 있으면 침입자가 로출될수 있는 위험성은 높아 진다. 위험도가 낮은 경우에는 이것이면 충분하다. 그러나 위험도나 위험요소가 증가되면 그것만으로는 안심할수 없다. 경비원의 주의가 딴데로 집중되면 사고가 누구도 모르게 일어 난다. 의심이 되는 경우에는 출입자신호장치가 없는 출입문의 밖에 카메라를 설치해 보아도 좋다. 자기들이 들어 오는것을 경비원이 보지도 못하며 문을 제꺽 열어 주지 않는다고 사람들은 불평할것이다. 카메라들은 경비원들의 눈(과 귀)의 확장으로서 정황을 평가하는데 가장 적합하다.

절도방지, 변경방지, 재고통제수단 콤퓨터와 말단장치들에 대한 절도행위가 자료의 리용성과 비밀성에 직접적영향을 미친다는것은 명백하다. 그러나 제마음대로 그 무엇을 변경시키는것도 자료의 무결성보장에 장애로 된다. 물리적으로 접근하게 되면 수많은 전통적인 IT보안조치들을 다 우회할수 있는 기회가 있으므로 모뎀, 무선망기판, 예비하드디스크를 끼워 통과암호파일을 훔칠수도 있으며 다른 OS를 기동시킬수도 있으며 비법적으로 망에 접근할수 있는 등 그 위험은 끝이 없다. 경로기 같은 보안장치들에 물리적으로 접근하여 현지에서 망에 접속하여 설정값들도 고쳐 놓을수 있다.

소매 및 도매기업들에서는 도난과 변경을 방지하는 굉장한 수의 제품들을 내놓았다. 변경방지장치들이 접근을 통제하여 보호자산의 무결성을 담보한다면 도난방지장치들과 재고품통제장치들은 제한지역에로의 움직임을 제한한다. 이 제품들의 기술은 지금까지 IT자산보호를 위한 새로운 제품들에 투하되여 왔다.

도난방지장치들에는 관건장치 달린 그물장, 서류함, 케스, 케블, 고정쇠들이 있다. 바코드(bar code) 같은 부표들과 재고통제수단들도 도난을 억제한다. 보다 정교한 장치들로는 진동수감기, 움직임수감기, 전원선감시체계, 전자상품감시(EAS)체계를 들수 있다. 전원선감시체계는 누가 콤퓨터나 기타 보호자산의 전원선을 뽑으면 경보가 울리게 되여 있는 장치이다. EAS체계는 보호자산이 해당 지역밖으로 나가면 경보가 울리는 장치이다. 가장 널리 알려 진 EAS장치들은 아마도 소매상점들에서 옷과 같은 기타 상품들에 달아 놓은 자그마한 딱지들일것이다. 판매원이 그 딱지의 기능을 정지시키지 않으면 상점밖으로 그것을 가지고 나갈 때 시끄러운 경보가 울리게 된다.

조작방지장치들로는 관건장치가 달린 서류장, 관건장치씌우개, 극소형스위치, 진동 및 운동수감부, 조작방지나사를 들수 있다.

물리적보안의 역할

물리적보안의 기본역할은 필요 없는 사람들을 들여 놓지 않으며 《내부사람》들을 언제나 정직하게 하는것이다. IT보안의 견지에서는 그 역할이 그리 다르지 않다. 물론 《사람》을 《사물》로 바꾸어 불, 물 등과 같은것으로 볼수도 있지만 기본사상은 다 같다. 가장 큰 차이라면 보호해야 할 재산의 범위가 넓은것이다. 물리적보안에서는 사람, 종이, 재산 등을 보호해야 할 뿐아니라 양식화된 자료들도 보호해야 한다.

그러면 무엇으로부터 시작할것인가. 앞에서 이미 언급된 계층적방어의 심도에 대한

해설을 상기해 보자(여기서는 하나의 장벽뒤에 또다른 장벽이 놓여 있다). 교과서에 있는 분석에 따르면 충분한 심도의 결정은 보안대응시간에 달려 있다고 한다. 물리적보안실천가들은 매개 통제수단 혹은 대응책을 하나의 시간지연행동으로 보고 있다. 경비력량이 동원되는데 걸리는 총시간이자 최소필요지연시간인것이다. 물론 물리적보안의 령역에서 많이 실천된 사실임에도 불구하고 이 지연전략은 극히 최근에야 IT보안전략의 하나로 제안되였다.

물리적세계에서의 작용은 다음과 같다. 가령 해당 지역 경찰로부터의 대응예상시간이 10분이라고 하자. 주변 울타리에는 경보장치가 없으므로 단순한 하나의 억제수단으로밖에 되지 않는다. 첫 경보기는 앞문에 있는데 앞문통과가 2분 걸리는것으로 본다. 그러면 경찰이 도적을 잡는데는 출입문과 현금사이의 내부계층들에 해당한 8분이라는 시간이 걸린다.

정보기술세계에서는 계층화라고 할 때 경로기가 뒤에 있고 대리자(proxy)가 뒤에 있는 방화벽들이 인차 떠오른다. 물리적통제수단들의 뒤에는 보충적인 물리적통제수단들이 또 있으며 싸이버통제수단들뒤에도 더 많은 싸이버통제수단들이 있다. 이것은 본질상 좋은것이다. 그러나 자료에 대한 보안에서는 물리적통제장치들과 싸이버통제장치들의 역할이 서로 보안적이여야 한다. 이것들이 다학과적인 방어에서 겹겹이 놓이는 격이다.

다학과적인 방어

다학과적인 방어에서는 보안문제를 해결하는데 하나이상의 기술이나 전문지식이 리용되게 된다. 물리적보안에는 장벽기술로부터 조작방지장치에 이르기까지 여러가지 학과 혹은 학문이 포괄되게 된다. 매 학문은 다른 학문에 도움을 준다. 매 요소는 하나의 목적을 가지고 다른 요소와의 협동밑에 사용된다. 매개 층에서 요소들사이의 기본관계는 보안사건을 방지하고 탐지하며 분석하려는 필요성이다. 실례로 경보접촉장치와 카메라가 달린 관건장치를 한 문이 있다고 하자. 그 문은 현재 사람들이 들어 가지 못하게 길을 막는 역할을 한다. 문이 열리면 경보신호가 울려 경비원을 부른다. 경비원은 카메라를 사용하여 정황을 분석하고 해당 대책을 세운다. 예방, 탐지, 분석에 여러가지 기술들이 집합적으로 리용된셈이다.

좀 더 넓은 견지에서 물리적보안을 하나의 학문으로, 정보기술보안도 하나의 학문으로 보자. 비록 서로 다른 학문이지만 이 두가지를 서로 분리하여 고찰할수는 없다. 실례로 로임과가 Windows NT를 쓰고 있다고 보자. 로임과장은 거기에 통과암호려파장치를 설치하여 모든 사용자들이 전적으로 담보되는 통과암호를 쓰게끔 하고 있다. 로임과장은 콤퓨터시동을 이동성매체(즉 플로피디스크나 CD–ROM)로도 할수 있기때문에 통과암호와 결국 망까지 위험성이 있다는것을 모르는바 아니다. 플로피디스크로 시동되기만 하면 통과암호파일들이 도난 당하거나 파괴 당할수 있다. 수많은 사람들이 회사에서 저녁늦게까지 일하며 제품을 생산하는 1층에서는 밤교대까지 있으나 로임과 직원들은 대체로 오후 4시면(로임지불전날을 제외하고) 다 퇴근한다.

한가지 방도는 플로피와 CD–ROM구동기를 다 떼버리는것이다. 그러나 이 제의는 경영진으로부터 그 일자리가 당신에게 귀중하지 않다면야… 하는 친절하나 확고한 경고에 부닥친다. 바이오스설정판에서 부트기능을 수정하고 스위치를 설치하고 마더보드에 있는 조작경보선택항목을 리용하여 조작방지용나사를 콤퓨터케스에 바꾸어 채운다. 이것은 다 학과적인 방법을 리용하는 하나의 실례이지만 의뢰기들의 수를 고려하면 특히 그 의뢰기들을 위한 봉사가 계속 진행되는 경우를 고려하면 추가적인 일감이 있게 되므로 그리 만족을 느끼지 못하게 된다. 그래서 물리적보안을 더 강구하여 하나의 또 다른 물리적보안층을 추가하는것이 좋다. 로임과 사무실에 있는 출입문에 보안성이 높은 막대기결쇠를 하나 채운다. 그래도 만족이 될가?! 경비체계가 있으면 경비원들에게 퇴근후 문이 정확히 닫기도록 하며 만일 누가 로임계산콤퓨터를 재시동시키거나 사용하는 사람이 있으면 다 기록해 놓으라고 강조하여 일러 둘수 있을것이다. 경비원이 누가 로임과 직원인지 혹은 담당직원인지 어떻게 안단말인가. 명단을 주면 될것이다. 이러한 보충적인 물리보안세부사항들은 대체로 잊고 있는 내용들이다.

이제는 반대의 위치에서 고찰해 보자. 새로운 카드출입체계(로임과와의 막후교섭의 결과인)에 상당히 만족하여 있는 경비원들과 한담을 하고 있다고 보자. 여러 기밀부서들에 들어 가는 사람들에 대한 통제권과 책임권은 그들에게 절대적으로 주어 져 있다. 로임과 사람들은 만족하며 로임관계정보도 안전하다고 본다. 설치만 하면 근심이 다 사라지는 이런 보안상 기발한 착상으로 물리적보안은 상당히 흐뭇하다. 경비원들도 그 수가 줄어 들었고 복도로 야간순찰하지 않아도 된다. 이때 한가지 생각이 계속 마음을 괴롭힌다. 이 카드출입체계의 콤퓨터가 어디에 놓여 있는가. 복도밑에 있는 작은 방에서 그 콤퓨터가 동작하고 있으며 그것도 Windows NT를 쓰며 통과암호관리자구좌도 없이 구좌검사도 없이 가동되고 있다는것을 인차 알게 된다. 음, 그러니까 콤퓨터귀신이면서도 불평이 많은 종업원이 로임파일들을 어쩌지 않는다고 아직도 담보할수 있는가?! 건물관리과에서 일하는 이전 경비원은 안전할가. 아마 현재 경비원으로 일하는 인원들에게 일정한 정보기술보안에 대한 방조를 줄 필요가 있다.

1996년에 채택된 《국가경제정탐관계법》을 보면 물리적으로나 전자적으로나 자료를 보호하는것이 가지는 중요성을 재인식할수 있다. 이 법은 외국정부가 리익을 보는 경우에 무역비밀의 도난이 정탐행위로 된다고 하였다. 그러나 《무역비밀》의 정의에는 다음과 같은 내용들이 포함되여 있다.

> 그 소유자는 이러한 정보를 비밀에 붙이기 위하여 합리적인 대책들을 취하였다. 그러나 현재 《합리적인 대책》이라는 말의 확고한 법적정의가 없으나 출발점으로 1997년 워싱톤특별시 FBI본부의 총무부 행정법률처 처장인 법률박사 패트릭 더블류 켈리는 자기 부문 요원들에게 다음과 같은 지침서를 하달하였다.《기업들에 건의하여 소유자들이 자기의 독점적인것이라고 간주되는 정보나 자료들은 명백히 표식하며 무역비밀이 보관되는 물리적재산들을 보호하며 직무상관계로 알아야 할 필요가 있는 인원에게만 무역비밀을 제한하며 회사의 무역비밀의 성격과 가치에 대하여 모든 종업원들에게 강습을 주기 위한 적극적인 대책들을 취하게 할것이다. 》

이것은 무역비밀이든 아니든 모든 귀중한 정보를 보호할수 있는 좋은 권고이다. 사실 켈리의 권고는 상식적인 보안내용이다. 이 상식적인 내용을 다음과 같이 묶어 볼수 있다. 즉 식별하라, 표식하라, 안전하게 하라, 추적하라, 알고 있으라이다. 이 분류는 보안조종의 실천적측면을 보여 준다. 물리보안을 위한 공통적인 실천사항들을 IT보안을 위한 실천사항들과 함께 아래에 제시한다.

1. 식별하라

ㄱ. **물리적보안** 정부는 이것을 분류지침이라고 한다. 무엇을 보호해야 하는가를 결정하고 제목별 혹은 주도어별로 그것을 어떻게 식별할것인가에 대한 지침을 작성하라. 그 지침만 있으면 신입사원이 내용에 기초하여 임의의 문건의 비밀성정도를 판정할수 있게 되여야 한다. 실례로 개발과제의 목적이나 의뢰자의 이름을 담은 그 어떤 문건은 《회사비밀》로 된다(그 개발과제이름은 기밀이 아니다).

ㄴ. **정보기술보안** 전자적인 분류지침을 작성하는것을 제외하고는 물리보안과 같다. 제목과 주도어별로 그것을 하이퍼링크하여 사용자가 몇가지 질문에만 대답을 주면 그 문건의 비밀성과 방책상 필요사항들을 쉽게 결정할수 있게 되여야 한다.

2. 표식하라

ㄱ. **물리적보안** 고무도장이나 붙임띠를 리용하여 기밀문건들을 표식해 두라. 문건철은 명백해야 하며(색갈로 혹은 색갈띠로 구분하여) 표식이 있어야 한다. 표식딱지에는 특별취급사항, 비밀성해제날자, 허용접근자 등에 대하여 명백히 지적되여 있어야 한다.

ㄴ. **정보기술보안** 기밀자료에 대하여서는 자동문건머리부/꼬리부나 표지를 리용하라. 인쇄시 자동적으로 표시페지가 찍혀 나오게 하라.

3. 보호하라

ㄱ. **물리적보안** 위험에 기초하여 물리적방어층을 구축하라. 다음의것들이 매 물리적보호들에 대한 가능성들이다. 결코 이것은 누구에게나 이것들이 다 필요하다는것이 아니다. 바깥층에서부터 안으로 들어 오는 이 보호층들은 정보기술보안실천자들이 반드시 알아야 할 물리보안층을 구성하는 공통적인 선택안들이다.

① **주변** 주변접근조종에는 울타리, 가시철조망, 정문, ID검열 등과 같은 물리적장벽들이 있다. 주변에서는 경보장치와 카메라도 리용된다.

② **건물마당** 건물마당안에서는 사람들(걸어 다니는 사람과 차를 타고 출입하는 사람들)의 출입을 통제하는 물리적장벽들과 함께 카메라, 조명, 경보장치, 순찰경비원 등이 배치될수 있다.

③ **건물의 입구** 출입문들, 관건장치들, 빗장을 지른 창문, 카메라, 경보기, 다

른 하나의 ID검열탁이나 카드접근체계(많은 호텔들에서 열쇠대신 카드를 리용하여 방에 들어 가듯이)가 있는 시설건물이 가까이에 있다.

④ **건물의 매층** 건물로 깊이 들어 갈수록 일부 호텔들처럼 승강기에 특별한 열쇠를 쓰며 계단들에 경보장치가 있는 등 층별로 접근이 더 제한된다. 계단층과 복도에는 감시카메라가 들어 있다.

⑤ **종합사무실** 종합사무실들에 대한 접근조종수단들에는 출입카드체계, 판건장치, 코드를 입력하는 번호판, 접수원, 쇠출입문 혹은 강심출입문이 있다. 나무로 만든 문들은 무게를 적게 하기 위해 속이 비였으므로 열기 쉽고 접철도 오래 간다. 그러나 철띠자물쇠와 같은 판건창치들을 설치하면 고정이 든든치 못하므로 인차 떨어 져 열릴수 있다. 단단한 심을 넣으면 문이 상당히 든든할수 있다. 종합사무실안에는 개별적인 사무실들이 있으며 거기로는 번호판, 카드, 보통열쇠 등을 리용하여 들어 갈수 있다.

⑥ **사무실물리보안** 사무실에 일단 들어 가면 판건장치가 있는 서류장, 금고, 금고실, 도난/조작방지용기구들, 경보체계 등이 있을수 있다. 기밀적인 디스크, CD–ROM들, 기타매체들은 다 장에 넣고 쇠를 채우라. 방화방수보관용기면 더욱 좋다. 서류처리기를 리용하라.

ㄴ. **정보기술보안** 위험에 기초하여 정보기술방어층을 형성하라. 방화벽, 대리자봉사기, 경로기, 망주소해석, 교환기, 망감시 등을 리용하라. 통과암호와 사용자인증을 리용하여 파일에 대한 접근권과 허용권, 항비루스, 자료여벌복사, 자료암호화, 덧쓰기편의프로그람 등을 리용하라. 창문에서 보이지 않는 곳에 모니터들을 놓으며 비상전원(UPS나 발전기), 예비설비를 두라.

4. 추적하라

ㄱ. **물리적보안** 접근목록(알고 있어야 할 목록), 기대점검목록, 재고품명세통제수단들, 재정검열, 등기우편 및 담보서한

ㄴ. **정보기술보안** 후열, 수자식인증서, 수자식서명, 파일사용허가 등

5. 알고 있으라

ㄱ. 물리적보안에서나 정보기술보안에서나 사람들이 무엇을 왜 해야 하는가를 잘 알도록 해야 한다. 보호실행을 위한 방책을 작성하라. 방책에는 필요한 접근조종대책들과 취급절차들이 명시되여야 한다. 직무에 따라 책임이 다르므로 그에 맞게 과제제시와 전습을 달리 적용하라.

ㄴ. **물리보안** 취급절차에는 복사, 우편보내기, 문서의 기밀기간, 문건페기 등에 대한 요구사항들이 담겨 져야 한다.

ㄷ. **정보기술보안** 전자적인 취급을 위한 방책들(례하면 복사, 절차, 전자우편보내기, Web싸이트에 게시하기, 파일지우기 등)이 마련되여야 한다.

물리적보안과 정보기술보안방책과의 통합

앞에서 본 《알고 있으라》부분의 기밀내용들을 만족시키기 위한 방책들이 세워 지면 기타 부분의 내용들을 실현할수 있는 필요한 로정도가 형성될수 있다. 매 부분에는 물리적보안의 실례들과 그에 대응되는 정보기술보안의 실례들도 언급되였다. 따라서 정보를 보호하기 위한 방책에는 물리보안요구사항들뿐아니라 정보기술보안요구사항들이 같이 취급되지 않으면 안된다. 수자식형태의 정보는 보호하면서 왜 종이형태의 정보는 보호하지 않겠는가. 방책에는 두 내용들이 다 담겨 져야 한다. 방법상 일관성은 있어야 하지만 응용에서 언제나 꼭같이 할 필요는 없을것이다. 실례로 개발계획에 대한 비밀정보가 안전하게 개발계획동업자들에게 전달되도록 하는 방책이 있다고 하자. 종이문서의 세계에서는 밀봉한 봉투에 넣은 문건이면 충분할것이다. 그러나 전자문서의 세계에서는 강력한 암호화가 필요하다. 봉투의 문건도 암호화하면 좋지 않은가, 물론이다. 배달원이 봉투를 뜯어 볼수 없으니까. 그래도 보호상태가 꼭같지 않단 말이지, 원인은 위험성의 규모에 있다. 배달원은 누구인가 고정되여 있고 담보도 있으며 만일 길가에 떨구었다 해도 그것을 주어 읽어 보는 사람은 매우 제한되여 있다. 그러나 인터네트망으로 보내면 누가 가운데서 접속해 읽어 보는지, 복사되는지, 다량으로 재배포되다가(그것도 무료로) 마침내는 어떤 나쁜놈의 손에 들어 가지나 않는지 도저히 알수 없게 된다. 《안전하게 하라》의 부분에서는 물리계나 전자계나 다 같다. 그러나 각기 실천에서는 개별적인 위험요소에 따라 구체적으로 적용되여야 한다.

방책의 전자적인 측면에서 볼 때 물리적접근조종을 떠나서는 절대로 그 무엇도 불가능하다. 실례로 높은 수준의 어느 방책에 이렇게 되여 있다고 하자. 《사용자들이 망접근권을 취득하자면 고유한 식별을 받아야 한다》. 이로부터 통과암호, 통과암호접수, 통과암호보관의 기준들이 제기되게 된다. 그러나 앞에서 든 어느 한 로임과의 실례에서 본바와 같이 높은 수준을 요구하는 방책의 성공은 그 방책에 콤퓨터에 대한 물리적접근의 보호를 위한 기준들을 포함시켜야만 가능한것이다. 그러므로 정보기술보안방책들과 기준들에 물리세계와 전자세계의 두 분야의 접근조종이라는 넓은 문제가 다 포괄되여야 한다. 이렇게 되여야 심도와 범위가 향상되게 된다. 기준과 방책이 전면적으로 구현되면 넓이도 잘 보장된다. 앞에서 본 로임과의 씨나리오에서 콤퓨터망전반에 걸쳐 기준들을 실행하였더라면 경보체계콤퓨터도 보호되였을것이다.

물리적보안의 함정

물리적보안을 실행함에 있어서 다음과 같은 일련의 제한성들과 약점들을 고려하여야 한다.

1. **사회공학** 정보기술보안에서와 마찬가지로 사회공학은 물리적보안통제수단을 교묘하게 잘 피한다. 흔히 해당 기관사람처럼 보이면 누구도 그의 신원을 묻지 않는

다. 그 사람이 그럴듯한 이야기를 꾸며 내면 경비원도 속히울수 있다. 낮시간접근통제용번호자물쇠와 전자카드열쇠체계도 출입을 금지하고 있을 때에는 잘못이 없지만 누군가가 속히워 자물쇠번호를 대주어 문이 열리게 할수도 있다.

2. **번호자물쇠의 약점** 통과암호와 같으므로 사람들은 흔히 자물쇠의 번호를 어디엔가 써놓거나 벽 같은데 붙여 놓을수 있다. 번호를 누를 때 어깨너머로 훔쳐 볼수도 있다.

3. **뒤따르기** 흔히 쓰는 수법이 뒤따르기하여 시설로 들어 가는것이다. 뒤따르기하려면 승인 받은 해당 인원이 들어 갈 때 뒤를 바싹 따라 가면 문이 닫기기전에 같이 들어 갈수 있다. 흔히 앞서 가는 사람은 뒤사람(즉 뒤따르는 자)을 위해 문을 붙잡아 주기까지 할수 있다. 무리 지어 들어 갈 때 따라 들어 가는것은 더욱 쉽다. 그들이 들어 갈 때 바쁜척하면서 초조해 하면 먼저 들어 가라고 양보해 줄수도 있다.

4. **날씨 및 환경조건** 날씨가 나쁘고 해가 너무 비치든가 반사가 있든가 안개 끼는 경우들에는 카메라가 쓸데 없으며 지어 수감부에서 허위경고를 낼수도 있다. 자동차시창이 더러운것처럼 카메라렌즈에 먼지나 때가 끼면 해를 볼때와 같은 산란현상이 있게 된다. 고열과 심한 추위도 설비들을 비정상적으로 동작시킬수 있다. 나무가지들이 자라나도 동물이나 새들처럼 주위의 경보장치들에 영향을 줄수 있다.

5. **실내전기제품들** 가열되거나 랭각되는 실내전기제품들은 움직임탐지기에 영향을 주며 허위경보를 울릴수 있다. 따라서 퇴근할 때에는 커피 끓이는 주전자나 가열판들의 전기스위치는 다 꺼야 한다. 움직이는 실내전기제품(선풍기 등)이나 설치물들(윙윙하는 창문빛가리개)도 더운 방에 찬바람이 불어 들어 올 때처럼 허위경보를 울릴수 있다. 랭동기의 압축기가 결함이 있어서 전기적인 잡음이 생기든가 방열기에서 김이 새는것과 같은 음향은 수감부들에 허위판단을 내릴수 있는 가능성을 줄수 있다.

6. **만성적인 태도** 장난군들에 의하여 우정 허위경보나 잘못된 경보가 울려 경보체계에 대한 신뢰도가 떨어 질수 있다. 실례로 진동수감부를 장치한 울타리를 탕하고 두들겨도 경보신호가 난다. 누구도 울타리를 타고 넘어 오지 않는다는것을 몇번 검열해 보고 난후에는 경보에 대해 인차 만성화된다. 또 오래동안 경보가 울리지 않으면 만성적인 태도가 생기거나 늦게야 반응하군 한다. 드문드문 훈련도 하고 경기도 조직하여 단조로움을 깨야 한다.

7. **비데오감시의 통지** 회사의 콤퓨터체계에 접속했을 때 사용자들에게 그들의 사적비밀보장이 부족하다고 통지해 주듯이 비데오감시를 늘 받고 있다는데 대하여서도 사람들에게 알려 주어야 한다. 카메라를 공개적인 장소에 설치할수 있는 법적근거와 관련하여서는 변호사와 토론하여야 한다.

8. **사용자들의 호응** 사용자들은 보안조치들이 너무 간섭적이며 힘들며 불안하다고 생각되는 경우에는 그 타당성정도에는 관계없이 불평할수도 있다. 의견이 많은 경우에는 사람들이 그것을 우정 마사 놓을수도 있으며 혹은 경영진자체가 그것을 없애라고 지시할수도 있다. 로조와도 사전합의를 보아야 할것이다. 로조에서 접수하지 않으면 다른 물리보안층을 생각해 내거나 매우 창조적인 사고를 해야 할것이다. 때로는 위험성이 접수될수 있는것으로 될지도 모른다.

정보기술과 물리적보안의 협동

협동이라는것은 서로의 요구를 리해하고 보완하기 위하여 리용되는것만은 아니다. 협동이란 자기가 남에게서 절대로 최우선적인 대우를 받지 못하리라는 리해로부터 출발한다는것을 의미한다. 서로의 우선사항에 없어서는 안될 존재로 되자면 어느 분야에 자기가 최적인가를 리해하기 위하여 노력하라. 그러한 사고방식으로 일하면 일정한 현실적인 발전이 이룩될수 있을것이다.

협동을 시작부터 잘하려면 방책에 이것이 잘 반영되여야 한다. 방책에는 물리보안팀과 보안관들의 특수한 역할과 책임관계가 명시되여야 할것이다. 방책들에 언명된 물리보안요구조건과 정보기술보안요구들을 비교해 보면 둘사이에 사건대응과 같은 공통적인 기초를 가진 분야들이 나타날수 있을것이다. 명백한 방책이 있든없든 교육, 협조, 실행이라는 세가지 요소들에 기초하여 협동을 진행해야 한다.

교육

물리보안실천가들인 보안설계가들과 보안관들을 초청하여 일정한 콤퓨터보안강습에 참가하게 하라. 그들을 IT세계에 끌어 들여 어느 부분에 가장 적합한가를 리해할수 있게 하라. 교실환경은 소감을 교환하고 IT실천가들의 사고방식에 다 적응되는 매우 좋은 장소이다. 그들을 학생으로서가 아니라 교사로 강습에 참가하게 하라. 교실에서 보는 관점과는 다른 독특한 관점을 제시할것이다. 전문보안관들은 그들이 흔히 맞다드는 문제인 반대의견에 부딪치면 매우 창조적인 생각을 내놓군 한다.

강의외에도 물리보안성원들에게 외부디스케트가 비루스를 끌어 들일수 있는 위험성이 있다는것, 기밀정보의 예비본테프가 도난 당할수도 있다는것과 같은 회사내의 IT관련 취약점들에 대하여 교육을 줄수 있을것이다. 이것이 나쁜것이니 회사전체의 리익을 다 말아 먹는다는 식으로만 이야기해 주지 말라. 구체적인 문제를 이야기해 주라. 어디에 바로 그러한 취약점이 있다는것을 찍어서 보여 주라. 가능하면 그 범죄를 저지시키는데 드는 소요시간과 그 범죄를 저지시키는데 어떤 자원을 리용하였는가 하는것까지 리해를 충분히 하도록 보여 주라. 실례로 어떤 시설에서 모뎀이 허용되지 않았다든가 어느 콤퓨터에서 조작체계를 파괴하자면 콤퓨터케스를 열어야 한다든가 하는것을 다 알려 주라. 그들에게 실지 모뎀이 어떻게 생겼는가를 망대면기판과의 비교속에서 보여 주어야 한다. 으시대지 말고 그들이 늘 쓰는 말로 설명하라. 즉 《전화기선을 꽂을수 있게 벽에 붙어있는 자그마한 꽂개를 알지요? 콤퓨터뒤부분에 있는 모뎀에는 그런것이 두개 달려 있습니다. 즉 하나는 전화기를 꽂는것이고 다른 하나는 전화선을 꽂는것입니다. 만약 그런 꽂개가 하나밖에 없으면 그것은 틀림없이 망기판입니다》.

협조

절차나 접근조종수단들을 개발하는 사업은 정보기술보안일군들과 물리보안일군들이

긴밀히 협조하면 그 질이 개선된다. 사용자들에게 일관성 있게 보이는 경우 사용자들이 더 도입하게 될것이다. 만약 기밀문건에 특별한 색갈로 표식을 하였다면 같은 문건의 전자본을 담은 디스케트에도 꼭같은 색갈로 표식하라. 기밀문건을 관건장치가 달린 서류함에 넣어야 한다면 전자본도 그와 같은 관건장치 있는 서류함에 보관하여야 한다.

협조는 또한 위험분석에도 도움을 준다. 계층적인 방어원칙들을 구현하는것은 상당히 복잡하며 때로는 비용이 상당히 들게 된다. 적중하고도 창조적인 물리보안을 설계하려면 위험관리훈련이 완성되여야 한다. 사실 물리보안실천자들은 예비봉사기와 같은 항목들의 진가를 리해하지 못할수도 있으므로 단순한 하드웨어교체의 가격으로 보기 쉽다. 예비봉사기에 회사자료가 담겨 져 있다면 이 봉사기가 대기(standby)상태에서 사용되고 있는중이라면 그 가치를 그저 하나의 하드웨어로만 보면 큰 실수일것이다. 한편 정보기술보안실천자들은 물리적보안통제수단들을 실행시키거나 교묘하게 피하는 창조적인 수법과 내부사람들의 절취범위에 대하여 잘 모를수 있다. 물리보안실천자들은 대체로 보안체계들의 원가나 실용성에 대하여 더 잘 알고 있다. 기관주변의 경보체계를 보고는 좋아하다가 정문에서 건물까지 차도밑에 케블을 깔아 늘이는데 얼마나 많은 자금이 들었는가를 썩 후에 알면 아마 다 놀랄것이다. 따라서 회사나 기관들이 물리보안관리자나 물리보안관을 한명 둘만큼 큰 경우에는 그 사람을 설치과정에까지 다 참가시키라. 위험평가전문회사를 사서 쓰거나 그러한 봉사를 제공하는 경우에는 보안관들중에 물리보안전문가가 한명이 있도록 하며 그들이 보안의뢰성원들과 상담하게 해야 한다. 취약점들과 비상봉사대응소요시간, 위험 등 데려 온 보안관들이 모르는것을 보안의뢰성원들은 현지에서 잘 알고 있을것이다.

협조에서 놓치지 말아야 할 문제들은 사건대응과 관련한 법률과 법조항들, 비상계획과 같은 문제들이다. 어떤 류형의 사건들을 대담하게 취급하며 어떤것을 낮은 수준에서 혹은 시간이 허락하면 취급할것인가에 대하여 합의를 보아야 한다. 어느 한 부서만 올리뛰고 내리 뛰고 하는데 다른 부서는 편안히 그 문제해결을 후에 보자는 식으로 할수는 없다. 이 단계에서 어느것을 먼저 하고 어느것을 후에 하겠는가를 식별해 내고 처리해야 한다. 예비봉사기를 도적 맞혔다 해도 거기에 자료도 없었고 또 망에 침입하지 않았다면 그 도난건은 정보기술과에 있어서 그리 중요한 문제가 아닐수도 있을것이다. 그러나 만일 그 도적이 방화출입문을 깨여 경보체계를 못쓰게 만들었다는것이 물리보안과에 의하여 발견되는 경우 이것은 생명안전과 관련되는 커다란 문제로 된다. 물리적보안과는 정보기술성원들에게 자기들이 어느것에 대한 조사와 실행을 먼저 추진해 나가겠는가에 대하여 통보해 주어야 한다. 그것은 봉사기가 있던 곳에 대한 증거문제에 영향을 줄수 있기때문이다. 이런 문제를 통보해 줄수 있는 방도를 잘 세워야 한다.

실행

협조할 때 결정된것들은 꼭 집행해야 한다. 그것을 시험해 보아서 어느것이 잘 안되는가를 보아야 한다. 그래도 안되는 일이 있으면 교육과 협조단계를 다시 거쳐 해결해야 한다. 실행과정에 대한 세밀조절은 지속적으로 해야 할 공정이다.

보충적인 정보

출발점으로 되는것은 산업보안협회(ASIS)이다. 주소는 www.asisonline.org이다. ASIS는 보안관리교육을 진흥시키는 단체로서 ASIS보호자격전문가(CPP)과정안을 제공한다. 그들의 Web페지에서는 많은 참고자료와 출판물들을 찾아 볼수 있다.

다른 하나의 기관은 해외보안자문리사회(OSAC)이다. 국무성에서 1985년에 설치한 이 OSAC는 정부와 해외에서 운영되는 사영부문과의 합영기관으로서 보안관계정보의 교환을 도모하고 있다. OSAC는 투자, 시설, 인원, 지적재산 등을 해외에서 보호하는데 필요한 정보를 제공한다. 보충적인 정보는 주소 www.ds–osac.org에서 볼수 있다.

물리보안상담역을 채용할 때에는 CCP자격이 있는가를 보며 그와 병행하여 IT분야에 경험이 있는가를 알아 보라. 정보기술보안과 물리보안 두 분야의 전문지식자격은 《정보체계보안전문가자격》(CISSP)이다. 상담역이 전문가자격이 없으면 그의 경험과 배경을 알아 보기 바란다. 련관 있는 좋은 경험과 배경에 전문자격까지 있으면 상당할것이다.

교육통계전국쎈터는 http://nces.ed.gov/pubs98/safetech/chapter5.html에 물리적보안에 관한 일련의 좋은 상식자료들과 검사대조목록을 제시하고 있다. 원래 학교들에서 사용할것으로 예견되였지만 많은 경우 상식자료들은 그 어느 분야에서도 적용할수 있다.

관건장치에 관심이 있다면 http://www.rc3.org/archive/inform/5/4.html에 좋은 기초자습본이 있으니 볼수 있을것이다. 현재는 발간되지 않는 이전 해커잡지 Informatik에는 기초적인 자물쇠류형과 그것을 깨는 방법들이 들어 있다. 10여년전의 잡지이므로 보안성이 높은 관건장치들은 취급되지 못했지만 간명하며 내용이 있다.

http://www.infosyssec.org/infosyssec/phyfacl.html에는 물리보안회사들과 물리보안관계정보들이 어지럼증이 날 지경으로 많이 목록화되여 있다. 물리보안을 시작하는 사람들이 여기부터 먼저 들릴 필요는 없다. 경험 있는 실천자들이 여기에서 해당 판매업체와 해당 정보를 찾으면 좋을것이다.

결 론

자료보호에서 난문제가 제기되였을 경우 현명한 IT보안관리자라면 물리보안전문가의 충고를 귀담아 들을것이다. 보안이 접근조종이며 보안은 계층화된 방어를 통해서만 최상의 효과를 달성할수 있다는것을 알아야 한다. 계층적인 방어에는 넓이, 길이, 억제라는 특징들이 있어서 모든 부분을 포괄하여야 하며 그 포괄범위는 예비적인 비상사태까지도 해당된다는것이다. 매 계층에 리용할수 있는 기술들은 상당히 많다. 보안상요구가 낮을 경우에 출입문에 관건장치나 하나 달아 놓는것으로 그칠수도 있지만 보호대상의 가치와 해당 위험요소가 클수록 보안상고려는 더욱 강조되여야 하는것이다. 탐지하고 분석할 겨를이 있는가, 억제가 1차적인 목적인가 등을 구체적으로 알아 보아야 한다. 그리고 자기 기관의 IT보안전략에서 취약적인 요소들이 어느 위치를 차지하며 그것들을 수정하거나 추켜 세우려면 보안전략에서 어느 부분을 고쳐야 하겠는가를 알아야 한다. 앞에서 본 5

가지 사항 즉 식별하라, 표식하라, 보호하라, 추적하라, 알고 있으라를 현존전략에 대한 검토나 새로운 전략작성에 리용하면 물리보안과 수자식보안이 서로 얼마나 보완적인가를 분석할수 있으며 나머지 미흡한 점들을 근원적으로 밝혀 낼수도 있을것이다. 그러나 물리보안전문가들과 수자식보안전문가들사이의 세부적인 협조와 합심이 없으면 실천적으로는 이 미흡한 점들은 정확히 제거되지 못할것이다. 그 호상관계들을 방책과 절차에 밝혀주어야 하며 호상 전습하는 사업에서 그 관계를 확립해야 한다. 자기 분야의 장점들과 특히 단점도 호상전습에서 밝혀야 한다. 잊지 말아야 할것은 물리보안이나 수자식보안이나 다같이 접근조종이라는 공동의 목적을 가진다. 이것을 달성하면 물리적으로나 수자식으로나 안전한 느낌을 가지고 공포와 의심에서 벗어 날수있을것이다.

참 고 문 헌

1. Winn Schwartau goes into great detail of detection versus reaction time for network security in his book *Time Based Security*, Interpact Press, Florida, 1999.
2. Kelly, Patrick W., J.D., LL.M., MBA *The Economic Espionage Act of 1996 Law Enforcement Bulletin* (July 1997), FBI Library, Washington, D.C., 1997.

색 인

ㄱ

ㄴ

ㄷ

ㄹ

ㅁ

ㅂ

ㅅ

ㅊ

ㅋ

ㅌ

ㅍ

ㅇ

A

B

N

O

P

R

S

T

U

V

W

X